



Defence Research and
Development Canada

Recherche et développement
pour la défense Canada



Investigation of Technologies and Techniques for Labelling Information Objects to Support Access Management

A. Magar

The scientific or technical validity of this Contract Report is entirely the responsibility of the contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada.

Defence R&D Canada – Ottawa

CONTRACT REPORT

DRDC Ottawa CR 2005-166

November 2005

Canada

Investigation of Technologies and Techniques for Labelling Information Objects to Support Access Management

A. Magar (Author)

Prepared by:

A. Magar Cinnabar Networks, Inc.
265 Carling Avenue
Ottawa, Ontario
K1S 2E7

Contract number: W7714-4-3115
Contract Scientific Authority: S. Zeber (613) 991-1388

The scientific or technical validity of this Contract Report is entirely the responsibility of the contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada

Defence R&D Canada – Ottawa

Contract Report
DRDC Ottawa CR 2005-166
November 2005

Principal Author

Original signed by

A. Magar

Information Security Architect

Approved by

Original signed by

S. Zeber

Defence Scientist

© Her Majesty the Queen as represented by the Minister of National Defence, 2005

© Sa Majesté la Reine, représentée par le ministre de la Défense nationale, 2005

Abstract

The Department of National Defence (DND) has a requirement to share information subject to need-to-know and security policy enforcement within a single network environment. The ability to bind a security label, containing classification and caveat information, to objects, in a secure and trusted manner, is a critical component of the access management infrastructure. This paper proposes an approach to security labelling suitable for the Secure Access Management for Secret Operational Networks (SAMSON) environment, that will allow security labels to be incorporated into all access decisions.

This page intentionally left blank.

Executive Summary

The Department of National Defence (DND) has a requirement to share information subject to need-to-know and security policy enforcement within a single network environment. The ability to bind a security label, containing classification and caveat information, to objects, in a secure and trusted manner, is a critical component of the access management infrastructure. This paper proposes an approach to security labelling suitable for the Secure Access Management for Secret Operational Networks (SAMSON) environment, that will allow security labels to be incorporated into all access decisions.

This paper defines security labelling as *information representing the sensitivity of a subject or object, such as its hierarchical classification (CONFIDENTIAL, SECRET, TOP SECRET) together with any applicable nonhierarchical security categories (e.g., sensitive compartmented information, critical nuclear weapon design information)*.¹ A security label can be deemed trusted if it is bound or linked to the object, such that this binding can later be validated by a third party. This binding is defined as a trusted process of inseparably associating one or more data items that can be validated by another party. The trusted process is typically accomplished using cryptographic techniques.

Although some research and development has been conducted into security labelling over the past thirty years, much of it as part of MultiLevel Security (MLS) initiatives, there is currently little commercial support for security labels and trusted binding mechanisms. Furthermore, no security labelling standard or trusted binding mechanism has emerged as a de-facto standard suitable for a variety of object classes. This will likely necessitate the use of a distinct security label and binding mechanism for each object class.

Based on the findings and conclusions reached during the development of this report, the following recommendations are made:

1. That SAMSON be used to explore and develop possible prototype solutions, with industrial collaboration where possible, for trusted labelling in a military environment; and
2. That the labelling strategy outlined in this report serve as the blueprint for trusted labelling within SAMSON.

¹ Infosec Glossary [13]

This page intentionally left blank.

Table of Contents

Abstract	i
Executive Summary.....	iii
Table of Contents	v
List of Figures	viii
Acknowledgements	ix
1. Introduction.....	1
1.1 Background	1
1.2 Purpose	2
1.3 Scope	2
1.4 Assumptions	2
2. Definition.....	3
2.1 Overview	3
2.2 Object Classes	3
2.3 Information Classification	4
2.3.1 Levels of Classification.....	4
2.3.2 Levels of Protection	4
2.3.3 Caveats	5
2.3.4 Need-to-Know.....	5
2.4 Security Policy.....	5
2.5 Access Control	6
2.5.1 Discretionary Access Control	6
2.5.2 Mandatory Access Control.....	6
2.5.3 Role-Based Access Control.....	7
2.5.4 Risk Adaptive Access Control	7
2.6 Security Label.....	7
2.6.1 Related Terminology.....	8
2.6.2 Labelling Approaches	8
2.6.3 Binding.....	9
2.6.4 XML-based Security Labels and Digital Signatures.....	9
2.7 Information Separation.....	10
2.7.1 DND Environment	11
2.7.2 Caveat Separation	12
2.7.3 MLS	13
3. Brief History	15
3.1 Overview	15
3.2 Bell-LaPadula Model	15
3.3 Biba Model	16

3.4	Trusted Computer System Evaluation Criteria	17
3.5	Information Technology Security Evaluation Criteria	18
3.6	Internet Protocol Security Option	18
3.7	Canadian Trusted Computer Product Evaluation Criteria	19
3.8	Security Label Framework for the Internet	19
3.9	FIPS 188 – Standard Security Label for Information Transfer	20
3.10	Dublin Core Metadata Initiative	21
3.11	Purple Penelope	21
3.12	Military Message Handling System	22
3.13	Security Architecture for the Internet Protocol	22
3.14	Common Criteria	23
3.15	DND Classified Workstation Security CONOP	24
3.16	NATO Labelling Directives	24
3.17	S/MIME Security Label	25
3.18	Controlled Access Program Coordination Office	26
3.19	French MOD Electronic Labelling Study.....	27
3.20	Global Information Grid	28
	3.20.1.1 Intelligence Community Markup Language	28
	3.20.1.2 DoD Discovery Metadata Specification	29
3.21	DND Metadata Application Profile	29
3.22	NC3A XSLs	30
4.	Commercial Approaches.....	33
4.1	Overview	33
4.2	Databases.....	33
4.3	Digital Rights Management.....	34
4.4	Messaging.....	34
4.5	Multilevel Network	35
4.6	Multilevel Operating Systems	35
5.	Requirements	37
5.1	Overview	37
5.2	Object & Application Support.....	37
	5.2.1 Object Classes	37
	5.2.2 Legacy Support	38
	5.2.3 SAMSON Applications.....	38
5.3	Structure	38
	5.3.1 Data Format.....	39
	5.3.2 Labelling Approaches	39
	5.3.3 XML-based Security Label and Digital Signature Type.....	40
5.4	Syntax	40

5.4.1	Classification.....	41
5.4.2	Caveat.....	41
5.4.3	Foreign Sensitivity	41
5.4.4	Security Policy	41
5.4.5	Access Rights.....	42
5.4.6	Expiration.....	42
5.4.7	Quality of Protection	42
5.5	Trust & Assurance	43
5.5.1	Binding Mechanism	43
5.5.2	Evaluation, Certification & Accreditation	44
5.6	General	44
5.6.1	Awareness	45
5.6.2	COTS	45
5.6.3	Interoperability.....	45
5.6.4	Translation	46
6.	SAMSON Security Labelling	47
6.1	Overview	47
6.2	Approach	47
6.2.1	Chat	49
6.2.2	Database	51
6.2.3	Documents	51
6.2.4	Email	52
6.2.5	Web Content	53
6.3	Strategy.....	53
6.3.1	Chat	53
6.3.2	Database	53
6.3.3	Documents	54
6.3.4	Email	55
6.3.5	Web Content	56
6.4	Level of Effort	57
6.5	Cost Estimate	58
7.	Conclusion & Recommendations	59
	References	61
	Annex A GIG IA Attributes	65
	Annex B DND MAP securityMarking Element.....	67
	Annex C Commercial Labelling Products.....	71
	List of symbols/abbreviations/acronyms/initialisms	79
	Glossary.....	83

List of Figures

Figure 1 - XML-based Security Labels and Digital Signatures	10
Figure 2 - Information Separation	11
Figure 3 - SAMSON Concept of Operations.....	12
Figure 4 - Security Labelling Timeline	15
Figure 5 - XML Security Container	27
Figure 6 - XSLS Prototype Architecture	31
Figure 7 - SAMSON Security Labelling Approach	48

Acknowledgements

The author would like to thank the following individuals for their expert advice and assistance during the preparation of this report.

- Dr. Steve Zeber, Defence Scientist, Information Operations Group, DRDC;
- Tim Moses, Director Advanced Security Technology, Entrust;
- Connie McFarland, Manager Software Development Content Analysis, Entrust;
- Andre Vellino, Senior Policy Architect, Entrust;
- John Hewie, Principal Account Technology Specialist, Microsoft Canada;
- Charlie Pulfer, General Manager, Titus; and
- Tim Upton, President, Titus.

However, any errors or inconsistencies found in this paper are the sole responsibility of the author.

This page intentionally left blank.

1. Introduction

1.1 Background

This paper continues a series of investigations into the application of Public Key Infrastructure (PKI), Privilege Management Infrastructure (PMI) and Identity Management (IdM) that began in 2000. Specifically, this Defence Research & Development Canada (DRDC) research initiative examines how these key technologies can be used to provide a caveat separation capability in the classified environment. This research initiative consists of the following milestones:

- PMI Investigation - In 2000 the Defence Research Establishment Ottawa (DREO), now DRDC, identified PMI as an area of information security relevant to the Department of National Defence (DND). An initial investigation was conducted into this technology and completed in March 2001 [1]. This work provided a broad overview of the technology as a whole and pinpointed some areas of particular interest to DND that were worthy of further research. In 2001, a second study examined the use of PMI technology in conjunction with PKI technology for the classified defence environment [2]. This work, which was completed in October 2001, proposed an architecture consisting primarily of Commercial-Off-The-Shelf (COTS) software.
- Secure Access Management Proof Of Concept (SAMPOC) I – A subsequent study prepared a complete project plan for a POC demonstration of a system combining COTS PMI, PKI and IdM technology to support information sharing subject to caveat separation in a classified defence environment [3]. This work, which was completed in June 2002, served as the blueprint from which the initial POC demonstration, SAMPOC I, was ultimately built. A follow-up report [4], released in December 2002, detailed the results of this initial POC and proposed a course for further research.
- Additional Research - In March of 2003, a survey of options for the policy server component was completed [5]. This was followed in July 2003 with a critical assessment of a Microsoft demonstration of a potential caveat separation solution [6].
- SAMPOC II – Based on this additional research, a new architecture, detailed design and project plan [7] was proposed that addressed much of the feedback received from SAMPOC I. SAMPOC II was implemented in the DRDC lab environment during the January to April 2004 timeframe. The results of this effort are fully documented in [8] and [9]. A portable version of SAMPOC II, built using laptop systems and virtual machine technology, was built in 2005 in order to provide a portable demonstration environment.
- Secure Access Management Secret Operational Network (SAMSON) Technology Demonstrator Project (TDP) – The success of this research, and SAMPOC II in particular, resulted in the creation of a DRDC TDP to develop this work further. The purpose of the SAMSON TDP is to develop and demonstrate a system in an operational environment capable of providing caveat separation within a single network environment that enforces security policy.

1.2 Purpose

DND has a requirement to share information subject to need-to-know and security policy enforcement within a single network environment. The ability to bind a security label, containing classification and caveat information, to objects, in a secure and trusted manner, is a critical component of the access management infrastructure. This paper proposes an approach to security labelling suitable for the SAMSON environment, that will allow security labels to be incorporated into all access decisions.

1.3 Scope

Labelling is an integral component of the information management process. Through the pervasive use of a labelling infrastructure, metadata can be used to facilitate information archiving and retrieval. While this aspect of labelling is of great importance, it is outside of the scope of this study. This report focuses exclusively on the use of security labels to facilitate information access, handling and protection.

1.4 Assumptions

It is assumed that the reader has at least a basic understanding of information security in general, and caveat separation in particular. Furthermore, this report makes the assumption that the reader has some familiarity with the SAMPOC demonstrators and the SAMSON TDP.

This paper also assumes that the industry partners who participated in the previous research initiatives will again prove instrumental in helping to deliver SAMSON. As a result, the proposed SAMSON security labelling solution attempts to leverage components from these vendors where possible.

2. Definition

2.1 Overview

In order to fully appreciate the subsequent discussion on security labelling it is important that the reader have a basic understanding of a number of relevant terms. These include an appreciation of object classes, information classification, security policy, access control, security labels and information separation.

2.2 Object Classes

Within a complex environment, such as the DND operational environment, there exist a great many objects to which access must be controlled. These include conventional objects such as documents, images and email messages, as well as less conventional objects such as chat sessions, video conferences, printers and web services. In order to better understand the specific security labelling requirements of certain objects, the objects have been organized into classes, where all of the objects in a given class have similar characteristics. The four object classes are as follows:²

- Information objects – *Information objects include any data file, report, document, photograph, database element, or similar types of data object. It might also include metadata that describes other objects. Information objects are arguably the core objects as they typically are what is being shared;*
- Service objects – *Service objects are executable applications that provide some function. They are the services in a service-oriented architecture. Service objects can be both active and passive objects of an access control decision;*
- Session objects – *Session objects are objects that are created as a result of a real-time interaction between two or more entities. A telephone call, a video teleconference, or an online virtual meeting, are examples of collaborative sessions that produce session objects; and*
- Real-time objects – *Real-time objects are a special class of information objects. Examples of real-time objects are live streaming video and voice, as well as real-time network management/control traffic exchanges. What makes real-time objects special is the temporal aspect of the objects (saving samples to disk turns real-time objects into normal information objects, i.e., these real-time objects are not retained to persistent storage media).³*

² The four classes of objects used throughout this report were taken from work being done as part of the Department of Defense (DoD) Global Information Grid (GIG). The GIG is discussed in some detail in Section 3.20 of this report.

³ GIG Information Assurance (IA) Capability/Technology Roadmap [10]

2.3 Information Classification

Within many security conscious organizations, objects are classified according to their sensitivity and the potential consequences of a security compromise. This is especially true within the federal government, which retains a great deal of military, intelligence and foreign policy information. Access to these sensitive objects is controlled in part based on the level of classification, level of protection, caveats and need-to-know restrictions assigned to these objects. Aside from national security information, information classification can also be used to protect personal information and intellectual property, and to facilitate access to information requests. Information classification includes levels of classification, levels of protection, caveats and need-to-know restrictions.

2.3.1 Levels of Classification

The level of classification is a hierarchical means to denote the sensitivity of an object. Of the four levels of classification used within the GoC, three are used in cases where the disclosure of the information could reasonably be expected to cause injury to the national interest. The four levels are as follows:

- **Unclassified** - Unclassified information is considered non-sensitive and in many cases may even be made publicly available;
- **Confidential** - *Confidential information is information related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause injury to the national interest;*
- **Secret** - *Secret is information is information related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause serious injury to the national interest; and*
- **Top Secret** - *Top Secret information is information related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause grave injury to the national interest.*⁴

2.3.2 Levels of Protection

The level of protection is a hierarchical means with which to denote *information related to other than the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause injury to a non-national interest.*⁵ The three levels of protection used within the GoC (Protected A, Protected B and Protected C) are used to represent the degree of potential injury (low, medium and high respectively) caused by the compromise of the information.

⁴ The definitions for Confidential, Secret and Top Secret are derived from the Government Security Policy (GSP) [11]

⁵ GSP [11]

2.3.3 Caveats

Classified information may be subject to further distribution and handling restrictions. These additional restrictions include warning terms or caveats, compartments and Community Of Interest (COI). Warning terms or caveats are used to indicate a nationality restriction (CEO, CANUS, CANUK, AUSCANZUKUS+, etc.) or restrict access based on distribution (e.g. NATO, K4, S4, etc.). For example, Secret information with the caveat CANUS is automatically restricted to Canadian and U.S. personnel with a Secret level clearance. Compartments limit information access based on the information type or source (e.g. Crypto Security, Warning Notice Intelligence Sources and Methods Involved, Atomal, etc.). COI are nonhierarchical groupings of sensitive information that provide a more granular means with which to restrict information dissemination to a given subset of users. The term caveat and COI will be used interchangeably throughout this report when referring to warning terms, caveats, compartments and COI.

For the purpose of this report, the term caveat is formally defined as *an attribute of an object that identifies it as belonging to some group of objects with one or more common characteristics. These characteristics can reflect the attributes that a user (a process) must have to access the object, or more commonly, special handling requirements.*⁶

2.3.4 Need-to-Know

Need-to-know is an even more granular, discretionary means with which to restrict information. A user may have the necessary clearance and belong to the appropriate COI, but may not have a need-to-know and thus be prevented from accessing the information. Need-to-know is defined as *the necessity for access to, or knowledge or possession of, specific information required to carry out official duties.*⁷ In other words, need-to-know is usually determined by the requirements of a functional role.

2.4 Security Policy

Security policy is defined as *the set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.*⁸ *The security policy is a set of high-level documents that state precisely what goals the protection mechanisms are to achieve. It is driven by our understanding of threats, and in turn drives our system design. Typical statements in a policy describe which subjects (e.g. users or processes) may access which objects (e.g. files or peripheral devices) and under which circumstances.*⁹

Within the Government of Canada (GoC), the GSP is a high-level security policy that *prescribes the application of safeguards to reduce the risk of injury. It is designed to protect employees, preserve the confidentiality, integrity, availability and value of assets, and assure the continued delivery of services. Since the Government of Canada relies extensively on information*

⁶ Lee [12]

⁷ Infosec Glossary [13]

⁸ Orange Book [14]

⁹ Security Policies [15]

*technology (IT) to provide its services, this policy emphasises the need for departments to monitor their electronic operations.*¹⁰ The GSP is supplemented by operational security standards intended to direct and guide the implementation of the policy. These operational security standards include the following:

- Organization and Administration;
- Physical Security;
- Management of Information Technology Security (MITS);
- Personnel Security;
- Contracting Management;
- Business Continuity Planning; and
- Operational Standard for the Security of Information Act.

2.5 Access Control

Access control is defined as *limiting access to information system resources only to authorized users, programs, processes, or other systems.*¹¹ Within information systems, access control services are used to enforce security policy. More specifically, they are used to dictate the circumstances under which a subject is entitled to access a sensitive object. Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC) and Risk Adaptive Access Control (RAdAC) are four distinct types of access control services. Access control services can be used individually or in combination.

2.5.1 Discretionary Access Control

DAC is defined as *a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).*¹²

*DAC, as the name implies, permits the granting and revoking of access privileges to be left to the discretion of the individual users. A DAC mechanism allows users to grant or revoke access to any of the objects under their control without the intercession of a system administrator.*¹³

2.5.2 Mandatory Access Control

MAC is defined as *a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization*

¹⁰ GSP [11]

¹¹ Infosec Glossary [13]

¹² Infosec Glossary [13]

¹³ Role-Based Access Control [16]

(i.e. clearance) of subjects to access information of such sensitivity.¹⁴ MAC is considered more secure than DAC due to the fact that the security policy is automatically enforced by the system and not left to the discretion of the users.

2.5.3 Role-Based Access Control

RBAC is defined as *a system of controlling which users have access to resources based on the role of the user. Access rights are grouped by role name, and access to resources is restricted to users who have been authorized to assume the associated role. Each user is assigned one or more roles, and each role is assigned one or more privileges to users in that role.*¹⁵

*RBAC bases access control decisions on the functions a user is allowed to perform within an organization. The users cannot pass access permissions on to other users at their discretion. This is a fundamental difference between RBAC and DAC. RBAC is in fact a form of mandatory access control, but it is not based on multilevel security requirements.*¹⁶

2.5.4 Risk Adaptive Access Control

RAAdAC is defined as *a rule-based access control policy based on real-time assessment of the operational need for access and the security risk associated with granting access.*¹⁷ RAAdAC is a relatively new development in the area of access control policy. It is meant to facilitate information sharing in military and security conscious government environments by incorporating security risk and operational risk as part of each access control decision. It is an integral component of the GIG architecture, discussed in Section 3.20.

2.6 Security Label

A security label is defined as *information representing the sensitivity of a subject or object, such as its hierarchical classification (CONFIDENTIAL, SECRET, TOP SECRET) together with any applicable nonhierarchical security categories (e.g., sensitive compartmented information, critical nuclear weapon design information).*¹⁸

This section will examine the following topics:

- Related Terminology;
- Labelling Approaches;
- Binding; and
- XML-based Security Labels and Digital Signatures.

¹⁴ Infosec Glossary [13]

¹⁵ Webopedia [17]

¹⁶ Role-Based Access Control [16]

¹⁷ GIG IA Capability/Technology Roadmap [10]

¹⁸ Infosec Glossary [13]

2.6.1 Related Terminology

In addition to the term security label, a variety of related terms are used in security literature. To prevent any confusion caused by the use of this related terminology, this paper will define these terms, including their use within this report:

- Metadata – Metadata is defined as *information about information. More specifically, information about the meaning of other data.*¹⁹ Metadata consists of a number of elements, and attributes within elements, to facilitate data discovery and sharing of information. In many cases a security label is either an attribute, or an element within an attribute, of a larger metadata schema. For the purpose of this report, metadata will be used to denote a general term encompassing data discovery and security label information. This use is consistent with that used by the Dublin Core Metadata Initiative (Section 3.10).
- Sensitivity Label – In most cases the term sensitivity label is used interchangeably with security label. However, in a number of instances the term sensitivity label is used to denote the confidentiality aspect of a security label. In order to simplify further discussion, the term sensitivity label will not be used within this report.
- Security Marking – In some cases the term security marking is used interchangeably with security label. However, in other instances it is used to refer to the human readable form of the security label. It is in this latter capacity that the term security marking will be used throughout this report.
- Tag – In many cases the term security tag is used interchangeably with security label. It is defined within the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) [19] as *a security attribute associated with an object. An object tag can be attached by the Trusted Computing Base (TCB) to a user, process or object.* In order to simplify further discussion, the term tag will not be used within this report.

2.6.2 Labelling Approaches

The two approaches to security labelling are as follows:

- Explicit Labelling - Explicit security labels consist of a number of bits designated for just this purpose. These bits are included with each labelled object (e.g., file, packet) in order to explicitly denote its security label.
- Implicit Labelling - Implicit security labels leverage an existing object attribute to convey security label information. For example, the use of a specific cryptographic key in a particular protocol can be used to determine the security label.

¹⁹ Dublin Core Metadata Initiative [18]

2.6.3 Binding

A security label can be deemed trusted if it is bound or linked to the object, such that this binding can later be validated by a third party. This binding is defined as a trusted process of inseparably associating one or more data items that can be validated by another party. The trusted process is typically accomplished using cryptographic techniques.

2.6.4 XML-based Security Labels and Digital Signatures

There are three types of XML-based security labels and digital signatures, which can be seen in Figure 1. They are as follows:

- Detached – A detached security label can be applied to data, including XML data, without modifying the structure of the data. Detached security labels are useful for labelling data that is not represented in XML or when labelling XML data without changing its structure. In order to bind detached security labels to an object, the computation of the signed digest value must include the digests of both the security label and the object. Similarly, detached digital signatures are applied over data that is external to the signature element.
- Enveloped – An enveloped security label is one which applies to its parent. In other words, the security label element is a child of the object element. Enveloped digital signatures are applied over data within the same XML document as the digital signature.
- Enveloping – An enveloping security label is one which applies to its children. In other words, the object element being labelled is under the security label element. Enveloping digital signatures are applied over data within the same XML document as the digital signature.

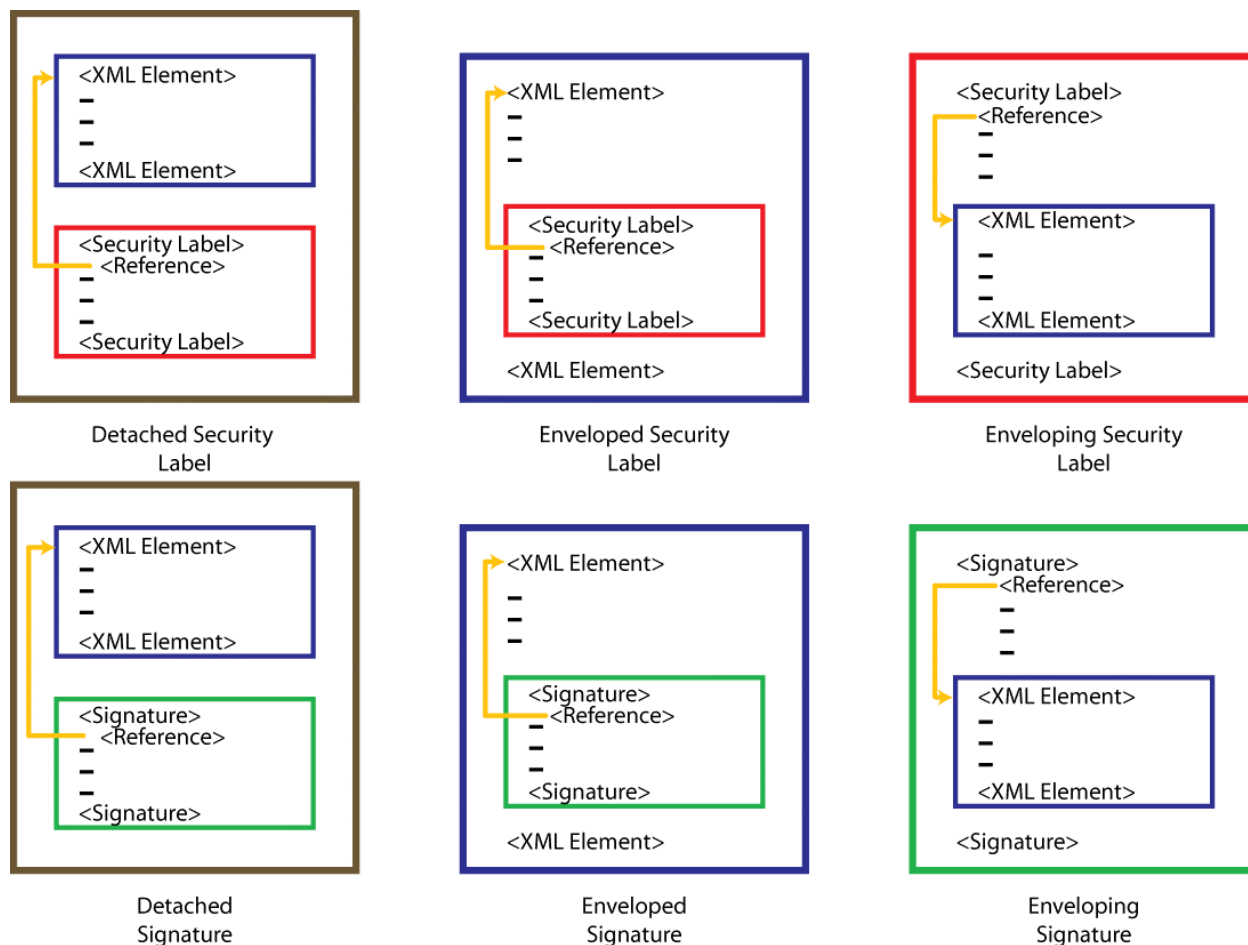


Figure 1 - XML-based Security Labels and Digital Signatures

2.7 Information Separation

How organizations ultimately control access to information, through the use of information classification, security policies, access control and security labelling, is termed information separation. Figure 2 illustrates three different approaches to information separation. The current DND environment is represented on the left, with caveat separation in the middle and MultiLevel Security (MLS) on the right. Although security labelling is an integral component of both caveat separation and MLS, the focus of this report will be on the use of security labelling as part of caveat separation.

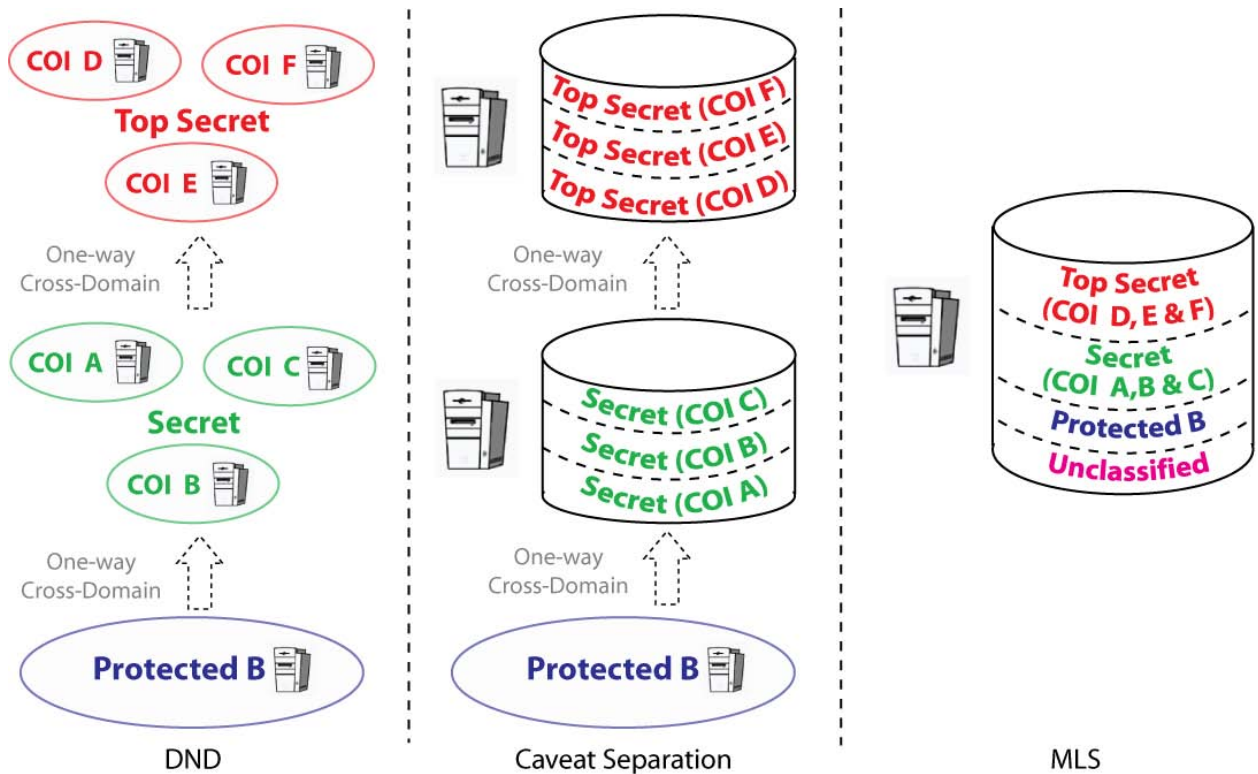


Figure 2 - Information Separation

2.7.1 DND Environment

DND has traditionally adopted a network-centric (netcentric) approach to information separation. It uses physically distinct networks to separate different classification levels and caveats. Each network in this environment operates in a “System High” mode, in which all personnel with access to the network must possess a security clearance higher than, or equal to, the highest security classification of information processed on the network. System high mode is formally defined as an *information system security mode of operation wherein each user, with direct or indirect access to the information system, its peripherals, remote terminals, or remote hosts, has all of the following: (a) valid security clearance for all information within an information system; (b) formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments and/or special access programs); and (c) valid need-to-know for some of the information contained within the information system.*²⁰

Physically separate networks are currently used in the DND classified environment to process information belonging to different caveats because the safeguards necessary to ensure caveat separation in a single network do not currently exist. An example is the TITAN network, which is

²⁰ Infosec Glossary [13]

classified SECRET CANUS. As both Canada and the US are NATO members, TITAN can host NATO information as well. However, information classified SECRET CEO cannot be hosted on TITAN, as this network lacks the necessary controls to provide caveat separation. As a result, SECRET CEO information must be held on a physically separate network.

2.7.2 Caveat Separation

Caveat separation allows multiple COI to be processed on a single network. However, separate networks are still required for each level of classification. As mentioned previously, sufficient security controls must exist in order to allow multiple caveats to be processed on a single network.

SAMSON proposes a new paradigm for managing access to information in a single network environment, through a number of independent safeguards that collectively enforce caveat and need-to-know separation, consistent with DND's defence-in-depth architecture. SAMSON consists of five integral components, that together form the basis for a caveat separation solution. These include strong authentication, policy-based authorization, trusted audit, centralized IdM and provisioning, and trusted labelling. These components can be seen in Figure 3. The concept behind SAMSON is loosely based on the idea of a reference monitor [20]. All attempts to access protected resources must be mediated by a policy function according to a centrally defined security policy.

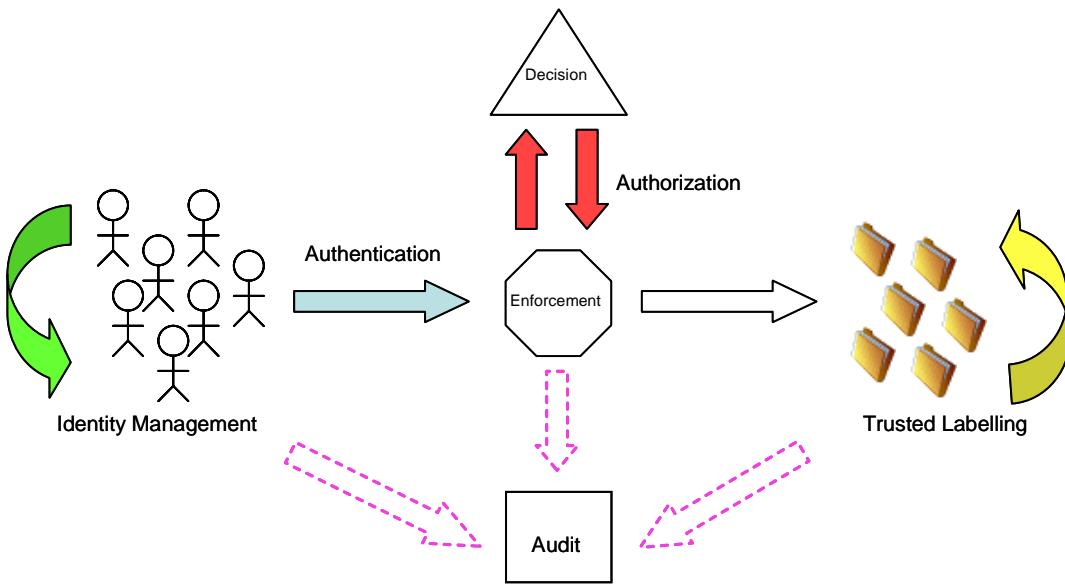


Figure 3 - SAMSON Concept of Operations

2.7.3 MLS

MLS was originally defined within the DOD-STD 5200.28, the National Computer Security Center's (NCSC) Orange Book [14] as *a class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users from obtaining access to information for which they lack authorization.*

Although this definition is accurate, for the purpose of this paper we will adopt the Department of Defense (DoD) Multilevel Security Program's [21] definition of MLS - *A capability that allows information with different sensitivities (i.e., classification and compartments) to be simultaneously stored and processed in an information system with users having different security clearances, authorizations, and needs to know, while preventing users from accessing information for which they are not cleared, do not have authorization, or do not have the need to know.*

MLS adopts a data-centric approach to information separation. Rather than necessitating physically distinct networks to separate different classification levels, MLS uses MAC to provide the appropriate level of information separation. These mandatory controls enable the network and systems to operate in multilevel mode. DAC are typically used to provide need-to-know separation in such an environment.

This page intentionally left blank.

3. Brief History

3.1 Overview

The concept of affixing a security label to an object in order to facilitate access mediation has evolved from its origins within the MLS research space. This section presents a number of milestones and seminal work in the evolution of security labels.

It is worth mentioning that the selection of these milestones is a subjective process. The work presented here is meant to represent a snapshot of the research completed over the past thirty years and can't possibly include all events of importance. It is also worth noting that the dates of these events are subject to interpretation as projects have start and end dates, while publications tend to have more than one version. Anyone interested in further information on the research discussed briefly in this section is encouraged to look at the references included with this report.

Figure 4 illustrates the evolution of security labels in the form of a timeline.

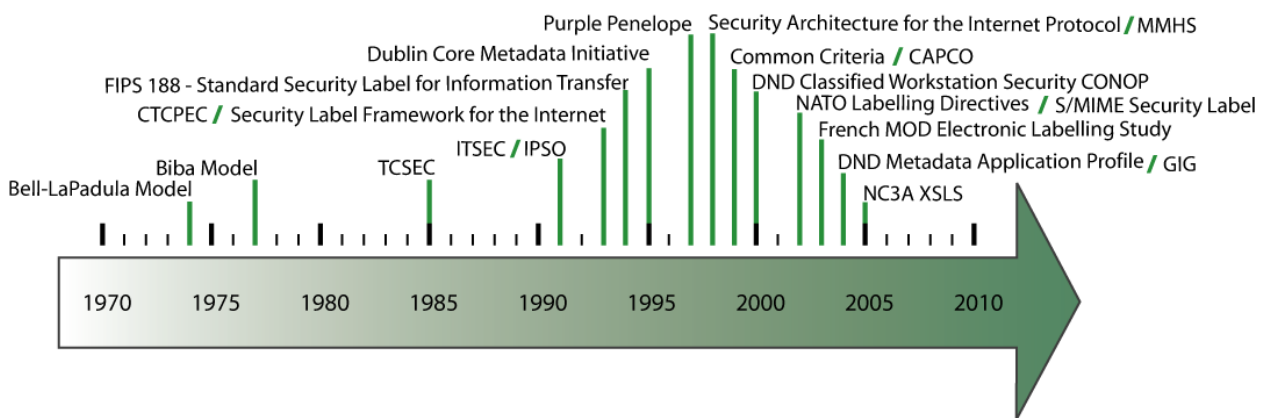


Figure 4 - Security Labelling Timeline

3.2 Bell-LaPadula Model ²¹

The Bell-LaPadula model is a representation of the confidentiality aspects of a security policy for conventional military security levels. Security policy is enforced within the Bell-LaPadula model through the use of two mandatory properties (the Simple Security Property (ss-property) and the *-Property), and one discretionary property (Discretionary Security Property (ds-property)).

²¹ Additional information on the Bell-LaPadula Model can be found in The Secure Computer System: Unified Exposition and Multics Interpretation [22]. This document was used to provide content for this section of the report.

The three properties are as follows:

- a. Simple Security Property - *The ss-property is satisfied if every “observe” access triple (subject, object, attribute) in the current access set b has the property that level (subject) dominates level (object). More concisely, the ss-property stipulates that if (subject, object, observe-attribute) is a current access, then level (subject) dominates level (object).* The ss-property, also called the ‘no read up property’, prevents subjects from reading objects whose classification exceeds their security clearance.
- b. *-Property - *The *-property is satisfied if: in any state, if a subject has simultaneous “observe” access to object-1 and “alter” access to object-2, then level (object-1) is dominated by level (object-2).* The *-property, also called the ‘no write down property’, prevents subjects, including malicious code, from leaking classified information to a lower level.
- c. ds-Property - *A state satisfies the ds-property provided every current access is permitted by the current access permission matrix M.* The ds-property allows subjects to share objects with other subjects provided that this does not contravene nondiscretionary security policy (ss-property and *-property).

The Bell-LaPadula model factors in the concept of a security level in its security policy. *The last component of a system state is a level function, the embodiment of security classifications in the model. In a military or government environment, people and documents can receive two types of formal security designations: one is classification or clearance (unclassified, confidential, secret and top secret are usual) and the other is formal category (such as Nuclear, NATO, and Crypto). A total security designation is a pair: (classification, set of categories). Such a pair we call a “security level”. A necessary condition for an individual’s possession of a document is that his security level must dominate the security level of the document.*

3.3 Biba Model ²²

The Biba Model is similar to the Bell-LaPadula in many respects, but its focus is on integrity in terms of access by subjects to objects, rather than confidentiality. The Biba model turns the Bell-LaPadula model upside down in order to prevent the corruption of ‘clean’ high level entities by ‘dirty’ low level entities. Security policy is enforced within the Biba model through the use of four integrity properties. The first two integrity properties are meant to prevent clean subjects and objects from being contaminated by dirty information in an environment where the integrity level never changes (static). The second two integrity properties automatically adjust the integrity level of an entity if it has come into contact with low-level information.

The four properties are as follows:

- a. Simple Integrity Property – This property, also called the ‘no write up property’, prevents subjects from moving low integrity data to high integrity environments.

²² Additional information on the Biba Model can be found in Integrity Considerations for Secure Computer Systems [23]. Computer Security [24] was used to provide content for this section of the report.

- b. Integrity *-Property – This property, also called the ‘no read down property’, prevents high integrity subjects from reading lower integrity objects.
- c. Subject Low Watermark Property – This property adjusts the integrity level of the subject accessing an object to the greatest lower bound of the integrity levels of the subject and object prior to the operation.
- d. Object Low Watermark Property – This property adjusts the integrity level of the object being accessed by a subject to the greatest lower bound of the integrity levels of the subject and object prior to the operation.

The Biba Model requires that subjects and objects are given an integrity label consisting of two parts; a classification and a set of categories or compartments. Integrity labels are meant to reflect the degree of confidence that can be placed in the data. In the Biba Model, integrity labels can either be static or dynamic. Dynamic labelling alters the integrity level to reflect changes in the degree of confidence that can be placed in the data.

3.4 Trusted Computer System Evaluation Criteria ²³

The DoD Trusted Computer System Evaluation Criteria (TCSEC) [14], or Orange Books as it is more commonly known, was published in December 1985 in order to *provide a basis for the evaluation of effectiveness of security controls built into automatic data processing system products.*

The Orange Book includes a discussion of six fundamental security requirements: *four deal with what needs to be provided to control access to information; and two deal with how one can obtain credible assurances that this is accomplished in a trusted computer system.* The second of these six requirements specifically addresses sensitivity labelling: *Requirement 2 - MARKING - Access control labels must be associated with objects. In order to control access to information stored in a computer, according to the rules of a mandatory security policy, it must be possible to mark every object with a label that reliably identifies the object's sensitivity level (e.g., classification), and/or the modes of access accorded those subjects who may potentially access the object.*

The criteria also specifies four divisions (D, C, B and A) and a number of classes of increasing assurance that the required features are operative, correct, and tamperproof under all circumstances is gained through progressively more rigorous analysis during the design process. Division B: Mandatory Protection specifies *the notion of a TCB that preserves the integrity of sensitivity labels and uses them to enforce a set of mandatory access control rules is a major requirement in this division. Systems in this division must carry the sensitivity labels with major data structures in the system. The system developer also provides the security policy model on which the TCB is based and furnishes a specification of the TCB. Evidence must be provided to demonstrate that the reference monitor concept has been implemented.* Class B1: Labeled Security Protection specifically addresses the requirement for labels and addresses such issues as

²³ The DoD TCSEC [14] was used to provide content for this section of the report.

label integrity and exportation of labelled information (exportation to multilevel devices, exportation to single-level devices and labelling human-readable output).

3.5 Information Technology Security Evaluation Criteria²⁴

The Information Technology Security Evaluation Criteria (ITSEC) [25] is the culmination of efforts to harmonise the security evaluation criteria of France, Germany, the Netherlands and the United Kingdom. *ITSEC is a structured set of criteria for evaluating computer security within products and systems. Each evaluation involves a detailed examination of IT security features culminating in comprehensive and informed functional and penetration testing. This work is undertaken using an agreed Security Target as the baseline for ensuring that a product or system meets its security specification. Seven evaluation levels are defined in respect of the confidence in the correctness of a Target of Evaluation (TOE). E0 designates the lowest level and E6 the highest.*

ITSEC proposes five example functionality classes derived from the functionality requirements of the hierarchical TCSEC classes. *Example class F-B1 is derived from the functionality requirements of the US TCSEC class B1. In addition to discretionary access control it introduces functions to maintain sensitivity labels and uses them to enforce a set of mandatory access control rules over all subjects and storage objects under its control. It is possible to accurately label exported information.*

3.6 Internet Protocol Security Option²⁵

RFC 1038 – Draft Revised IP Security Option [26] was drafted in January of 1988. It was superseded by RFC 1108 – Security Options for the Internet Protocol [27], which was completed in November of 1991. These standards are collectively referred to as the Internet Protocol Security Option (IPSO). IPSO was designed to support the security labels in use by the U.S. DoD. IPSO spawned a commercial equivalent, the Commercial Internet Protocol Security Option (CIPSO), intended for use in commercial, U.S. civilian and non-U.S. communities. IPSO is explicit, in that the security label consists of actual bits in the protocol control information. It is also connectionless, in that the security label appears in every Protocol Data Unit (PDU).

IPSO defines two DoD security options:

- DoD Basic Security - *This option identifies the U.S. classification level at which the datagram is to be protected and the authorities whose protection rules apply to each datagram.*
- DoD Extended Security - *This option permits additional security labelling information, beyond that present in the Basic Security Option, to be supplied in an IP datagram to meet the needs of registered authorities.*

²⁴ The ITSEC [25] was originally published in May 1990 and then updated (version 1.2) in June 1991. The updated document was used to provide content for this section of the report.

²⁵ RFC 1108 – Security Options for the Internet Protocol [27] was used to provide content for this section of the report.

3.7 Canadian Trusted Computer Product Evaluation Criteria²⁶

The CTCPEC [19] presents *a set of technical hardware/firmware/software criteria for trusted products which is consistent with the Security Policy of the Government of Canada, the Information Technology Security Standards under development by the Government of Canada and takes into account reciprocity issues with technical criteria of other nations strategically allied with the Government of Canada. The criteria have been developed to provide:*

- *the Government of Canada with a metric with which to evaluate the degree of assurance that can be placed in computer products used for the processing of sensitive information;*
- *a guide to manufacturers as to what security services to build into their commercial products in order to produce widely available products that satisfy requirements for sensitive applications; and*
- *a guide which may be used in procurements of trusted products.*

The criteria is a metric used for the evaluation of the effectiveness of the security services provided by a product by splitting the Criteria into two distinct groups known as the duality of functionality and assurance. Functionality consists of Confidentiality, Integrity, Availability, and Accountability Criteria. The Assurance Criteria, on the other hand, reflect the degree of confidence that a product correctly implements its security policy.

The term tag is used pervasively throughout the CTCPEC, most notably in discussions on discretionary confidentiality services, discretionary integrity services, mandatory confidentiality services and mandatory integrity services. *A tag is a security attribute associated with an object. An object tag can be attached by the TCB to a user, process or object.*

3.8 Security Label Framework for the Internet²⁷

RFC 1457 – Security Label Framework for the Internet [28] was published in May 1993. Not only does this RFC attempt to define a number of terms (security label, integrity label and sensitivity label), but it examines security label usage, approaches to labelling and labelling within the Open Systems Interconnection (OSI) reference model.

In data communication protocols, security labels tell the protocol processing how to handle the data transferred between two systems. That is, the security label indicates what measures need to be taken to preserve the condition of security. Integrity labels are security labels which support data integrity models, like the Biba model. The integrity label tells the degree of confidence that may be placed in the data and also indicates which measures the data requires for protection from modification and destruction. Sensitivity labels are security labels which support data confidentiality models, like the Bell and LaPadula model. The sensitivity label tells the amount of damage that will result from the disclosure of the data and also indicates which measures the

²⁶ While the first version of the CTCPEC was released in 1989 and the second in 1990, the third and final version [19] wasn't published until January of 1993. This document was used to provide content for this section of the report.

²⁷ RFC 1457 – Security Label Framework for the Internet [28] was used to provide content for this section of the report.

data requires for protection from disclosure. The amount of damage that results from unauthorized disclosure depends on who obtains the data; the sensitivity label should reflect the worst case.

The RFC defines two approaches to security label usage:

- *End System Security Label Usage - When two end systems communicate, common security label syntax and semantics are needed. The security label, as an attribute of the data, indicates what measures need to be taken to preserve the condition of security. The security label must communicate all of the integrity and confidentiality handling requirements. These requirements can become very complex.*
- *Intermediate System Security Label Usage - Intermediate systems may make routing choices or discard traffic based on the security label. The security label used by the intermediate system should contain only enough information to make the routing/discard decision and may be a subset of the security label used by the end system. Some portions of the label may not effect routing decisions, but they may effect processing done within the end system.*

3.9 FIPS 188 – Standard Security Label for Information Transfer²⁸

Federal Information Processing Standards (FIPS) 188 – Standard Security Label for Information Transfer [29] was published in September 1994 in order to define a security label syntax for information exchanged over data networks and provides label encodings for use at the Application and Network Layers. This standard defines syntactic constructs for conveying security label information when Government sensitive but unclassified data is exchanged over computer networks. Although this standard is intended for use on systems handling unclassified information, it could be adopted by the appropriate authorities for use on systems handling classified information.

Security labels convey information used by protocol entities to determine how to handle data communicated between open systems. Information on a security label can be used to control access, specify protective measures, and determine additional handling restrictions required by a communications security policy. The label presented here defines security tags that may be combined into tag sets to carry security-related information. Five basic security tag types allow security information to be represented as bit maps, attribute enumerations, attribute range selections, hierarchical security levels, or as user-defined data. Because of inherent differences in layer functionality, the security label defined in this document is expressed both as an abstract label syntax specification for the OSI Application Layer and an encoding optimized for use at the Network Layer.

²⁸ FIPS Pub 188 – Standard Security Label for Information Transfer [29] was used to provide content for this section of the report.

3.10 Dublin Core Metadata Initiative²⁹

The Dublin Core Metadata Initiative (DCMI) *is an open forum engaged in the development of interoperable online metadata standards that support a broad range of purposes and business models. DCMI's activities include consensus-driven working groups, global conferences and workshops, standards liaison, and educational efforts to promote widespread acceptance of metadata standards and practices.*

Although the DCMI was established in 1995, the Government Working Group wasn't convened until 1999. *The DC-Government Working Group is a forum for individuals involved in implementing Dublin Core within and between government agencies and International Government Organizations (IGO's).*

The DCMI does not have a security label element. However, it does have a Rights element and the DC-Government Working Group has proposed extending this to include a Security Classification qualifier. This qualifier is defined as *the classification allocated to the resource indicating its official security status or other restrictions on its availability. The purpose of this qualifier is to facilitate proper and appropriate management of sensitive or security classified records.*

3.11 Purple Penelope³⁰

Purple Penelope was a prototype implementation of a secure labelling system for Windows NT3.51. It was originally produced by the Defence Research Agency (DERA) as part of the UK Ministry Of Defence (MOD) Applied Research Program. The software was eventually licensed to Argus Systems where it was developed into a product called Deep Purple.

The objective of the project was *to show that the security functionality of Windows NT can be extended to provide labelling, and other security mechanisms, which support users who must handle sensitive information. This is despite the fact that NT does not provide any direct support for labelling functionality.* Purple Penelope was intended for use in system high or compartmented mode domains as it was deemed inadequate for multilevel use.

Within Purple Penelope, security marking information, which is applied to all files and applications, is displayed in a stripe across the top of the screen. The content of the stripe depends on the application that is active at the time. *As applications read files, the application's label floats up according to the label of the file that is read. Similarly, when an application writes a (private) file, the file's label floats up according to the label of the application. An application may, however, lower its label at any time, although many applications will only do this when requested to do so by the user. A common mechanism is provided through which the user can request the application to change the label of the selected data. A mouse-click on the marking displayed in the screen stripe brings up a choose-marking dialogue with which the user can select a new marking. When an application copies data into the clipboard, the clipboard label is set to*

²⁹ The Dublin Core web site [18] was used to provide content for this section of the report.

³⁰ Purple Penelope: Extending the Security of Windows NT [30] and *A New Strategy for COTS in Classified Systems* [31] were used to provide content for this section of the report.

that of the application. When an application takes data from the clipboard, the application label floats according to the clipboard label. The clipboard label can be changed at any time, most easily by clicking on the clipboard marking displayed in the screen stripe. This gives the user a convenient way of extracting data which warrants a low marking from a document that overall has a high marking.

3.12 Military Message Handling System ³¹

The DND Military Message Handling System (MMHS) is capable of supporting the exchange of Unclassified, Designated and Classified message traffic. This new electronic messaging system is a Defence Service Program (DSP) project referred to as the Defence Message Handling System (DMHS). The Military Message Handling System (MMHS) portion of the DMHS is designed to replace the existing national strategic messaging network known as the Automated Defence Data Network (ADDN) and is intended to handle Unclassified, Designated and Classified military messaging traffic up to and including Secret.

MMHS will be implemented as a SECRET system-high capability which will support message security labeling, (e.g., Secret, Confidential, Protected A, Canadian Eyes Only (CEO), etc.) utilized by the current legacy systems (e.g., the ADDN). Specifically, all traffic handled within the MMHS domain will be treated as SECRET, but originator assigned message security labels will also be supported to indicate the complete access control requirement for each message. This will facilitate the ability to automatically screen message traffic flowing from the MMHS to external networks and it will indicate the appropriate handling restrictions associated with each message.

Besides the classification (mandatory), security labels include security policy identifiers (mandatory), categories (optional) and privacy marks (optional). A message security label includes one policy identifier, one classification, zero or more categories (permissive, restrictive, and or informative), and optionally a privacy mark.

3.13 Security Architecture for the Internet Protocol ³²

RFC 2401 – Security Architecture for the Internet Protocol [34] was published in November 1998 and specifies the base architecture for IPsec compliant systems. The goal of the architecture is to provide various security services for traffic at the IP layer, in both the IPv4 and IPv6 environments.

Unlike its predecessor, IPv6 did not originally have any explicit labeling. In fact, RFC 2401 foundation specification only suggested that implicit labeling be used with IPv6 packets - by creating a separate IPsec security association per label. The RFC 2401 draft addressed the limitations of the implicit labeling schema and proposed a generalized labeled security option to be used in a hop-by-hop or destination extension header of the IPv6 packet.

³¹ MMHS System Concept of Operations [32] and MMHS Concept of Operations: The User's Perspective [33] were used to provide content for this section of the report.

³² RFC 2401 – Security Architecture for the Internet Protocol [34] was used to provide content for this section of the report.

The Authentication Header can be used to provide strong assurance for both mandatory access control decisions in multi-level networks and discretionary access control decisions in all kinds of networks. If explicit IP sensitivity information (e.g., IPSO) is used and confidentiality is not considered necessary within the particular operational environment, the Authentication Header can be used to provide authentication for the entire packet, including cryptographic binding of the sensitivity information to the IP header and user data. This is a significant improvement over labeled IPv4 networks where the sensitivity information is trusted even though there is no authentication or cryptographic binding of the information to the IP header and user data. IPv4 networks might or might not use explicit labelling. IPv6 will normally use implicit sensitivity information that is part of the IPsec Security Association but not transmitted with each packet instead of using explicit sensitivity information. All explicit IP sensitivity information MUST be authenticated using either ESP, AH, or both.

3.14 Common Criteria³³

The Common Criteria for Information Technology Security Evaluation [35], hereafter referred to as the Common Criteria, is the result of the harmonization of a number of different evaluation criteria developed throughout the world. These include the Canadian CTCPEC, the European ITSEC and the U.S. TCSEC.

Common Criteria evaluations include both a Protection Profile (PP) and an Evaluation Assurance Level (EAL). *A protection profile defines an implementation-independent set of security requirements and objectives for a category of products or systems which meet similar consumer needs for IT security. A PP is intended to be reusable and to define requirements which are known to be useful and effective in meeting the identified objectives.* At the time of writing 45 distinct PPs had been developed. The seven EALs defined in the Common Criteria are a hierarchical representation of the level of assurance that can be placed in the product or system.

The Common Criteria Labelled Security Protection Profile [36], hereafter called *LSPP*, specifies a set of security functional and assurance requirements for Information Technology (IT) products. *LSPP conformant products support access controls that are capable of enforcing access limitations on individual users and data objects. Specifically, two classes of access control mechanisms are provided: those that allow individual users to specify how resources (e.g., files, directories) under their control are to be shared; and those that enforce limitations on sharing among users. The latter is implemented by the use of security markings (i.e., “labels”).*

The LSPP was derived from the requirements of the B1 class of the U.S. Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC), dated December, 1985, and the material upon which those requirements are based. This protection profile provides security functions and assurances which are equivalent to those provided by the TCSEC and replaces the requirements used for B1 trusted product evaluations.

³³ The Common Criteria for Information Technology Security Evaluation [35] was published in August of 1999. However, it was the Common Criteria Labelled Security Protection Profile [36] that was used to provide content for this section of the report.

3.15 DND Classified Workstation Security CONOP ³⁴

The DND Classified Workstation Security Concept of Operations [37] was published in January 2000 by the Director Distributed Computing Engineering and Integration (DDCEI). It includes an overview, in terms of security labelling, of classifications, designations, warning terms, restricted handling terms, special handling designators and nationality restrictions.

The structure of the label is primarily intended to meet the requirements of automated access control checks to be implemented in MMHS messaging components, but the same structure and contents should be used manually throughout the classified domain, except where existing paper-based labelling conventions preclude it. The security label is composed of four fields as follows:

- a. Security Policy Identifier. Indicates the security policy in force to which the security label relates. The policy identifiers that shall be supported are Government of Canada, NATO and CCEB. Although each identifier represents a different security policy, all three identifiers may be used in the DND classified messaging environment depending upon the ultimate audience for the message. Thus it may be correct to initiate messages for DND internal recipients using the GoC policy identifier on the same workstation as messages for NATO recipients using the NATO policy identifier;*
- b. Security Classification. Indicates the classification of the object in the hierarchical set of security classifications, indicating the degree to which the object is sensitive in the national interest;*
- c. Privacy Mark. A user defined label. Examples of user defined labels that can be placed here are EXERCISE, OFF-LINE ENCRYPTED, RESTRICTED FOR XXX, etc; and*
- d. Security Category. Indicates the specific security category or categories associated with the object. Multiple security categories are supported per label, up to a maximum of 64.*

3.16 NATO Labelling Directives ³⁵

The Infosec Technical Directive for Labelling of NATO Information in Electronic Format [38] and Electronic Labelling of NATO Information [39] were published in September 2001 and October 2002 respectively. These NATO labelling directives establish requirements for attaching sensitivity labels to NATO information in electronic format.

³⁴ The DND Classified Workstation Security Concept of Operations [37] was used to provide content for this section of the report.

³⁵ The Infosec Technical Directive for Labelling of NATO Information in Electronic Format [38] and Electronic Labelling of NATO Information [39] were used to provide the content for this section of the report.

Attaching a label to electronic information is one mechanism for enabling the protection of information. It promotes originator awareness of the requirement for correct and consistent marking, facilitates automated access and release control, enables the use of multi-level security systems, and removes the need to thoroughly examine electronic information in order to determine its sensitivity. Properly and carefully constructed, electronic labels can be efficient, unambiguous, and faithfully reflect the security policy of which they are an instance. These properties make electronic data labels ideal for protecting information in wide-area, multinational, high traffic applications.

A sensitivity label is an assertion of the sensitivity of a piece of information that is bound to the information. In the paper environment, this is a marking, usually at the top of a page. It expresses in words the protection to be afforded the document. In a computing environment, it is a piece of electronic data that has been encoded to represent the same sensitivities as in the paper environment. This electronic label can be used to limit access to information, to ensure that information is transmitted in appropriate ways, and to enable appropriate output markings.

3.17 S/MIME Security Label ³⁶

RFC 2634 – Enhanced Security Services for S/MIME [40] and RFC 3114 - Implementing Company Classification Policy with the S/MIME Security Policy [41] were drafted in June 1999 and May 2002 respectively. RFC 2634 describes four optional security service extensions for S/MIME, including security labels. RFC 3114 discusses how company security policy for data classification can be mapped to the S/MIME security label.

*A security label is a set of security information regarding the sensitivity of the content that is protected by S/MIME encapsulation. The sensitivity information in a security label can be compared with a user's authorizations to determine if the user is allowed to access the content that is protected by S/MIME encapsulation. Security labels may be used for other purposes such as a source of routing information. The labels often describe ranked levels ("secret", "confidential", "restricted", and so on) or are role-based, describing which kind of people can see the information ("patient's health-care team", "medical billing agents", "unrestricted", and so on). Integrity and authentication security services **MUST** be applied to the security label, therefore it **MUST** be included as a signed attribute, if used.*

S/MIME security label components include the following:

- Security Policy Identifier – *A security policy is a set of criteria for the provision of security services. The `eSSSecurityLabel` security-policy-identifier is used to identify the security policy in force to which the security label relates. It indicates the semantics of the other security label components.*
- Security Classification - *If present, a security-classification may have one of a hierarchical list of values. The basic security-classification hierarchy is defined in this Recommendation, but the use of these values is defined by the security-policy in force. Additional values of security-classification, and their position in the hierarchy, may also be*

³⁶ RFC 2634 – Enhanced Security Services for S/MIME [40] and RFC 3114 - Implementing Company Classification Policy with the S/MIME Security Policy [41] were used to provide the content for this section of the report.

defined by a security-policy as a local matter or by bilateral agreement. The basic security-classification hierarchy is, in ascending order: unmarked, unclassified, restricted, confidential, secret, top-secret.

- *Privacy Mark - If present, the eSSSecurityLabel privacy-mark is not used for access control. The content of the eSSSecurityLabel privacy-mark may be defined by the security policy in force (identified by the eSSSecurityLabel security-policy-identifier) which may define a list of values to be used. Alternately, the value may be determined by the originator of the security-label.*
- *Security Categories - If present, the eSSSecurityLabel security-categories provide further granularity for the sensitivity of the message. The security policy in force (identified by the eSSSecurityLabel security-policy-identifier) is used to indicate the syntaxes that are allowed to be present in the eSSSecurityLabel security-categories. Alternately, the security-categories and their values may be defined by bilateral agreement.*
- *Equivalent Security Labels - Because organizations are allowed to define their own security policies, many different security policies will exist. Some organizations may wish to create equivalencies between their security policies with the security policies of other organizations.*

A security label can be included in the signed attributes of any SignedData object. A security label attribute may be included in either the inner signature, outer signature, or both.

3.18 Controlled Access Program Coordination Office ³⁷

Controlled Access Program Coordination Office (CAPCO) is a classification marking system developed for the U.S. intelligence community. It *uses a uniform list of security classification and control markings authorized for all dissemination of classified information by components of the intelligence community.* CAPCO consists of the following seven categories of classification and control markings:

- **Classification** – There are four levels of classification; Top Secret, Secret, Confidential and Unclassified.
- **Non-U.S. Classification Markings** – This category contains classification markings used by other countries and international organizations.
- **Sensitive Compartmented Information (SCI) Control System Markings** – SCI Control System Markings are *the system of procedural protective mechanisms used to regulate or guide each program established by the Director of Central Intelligence as SCI. A control system provides the ability to exercise restraint, direction, or influence over or provide that degree of access control or physical protection necessary to regulate, handle or manage information or items within an approved program.*
- **Foreign Government Information** – Foreign Government Information markings are used in U.S. controlled documents which contain controlled information of non-U.S. origin.

³⁷ Intelligence Community Classification and Control Markings Implementation Manual [42] was used to provide the content for this section of the report.

- Dissemination Controls – Dissemination Controls are control markings which identify the expansion or limitation on the distribution of information.
- Non-Intelligence Community Markings – Non-Intelligence Community Markings are markings authorized for use by entities outside of the Intelligence Community.
- Declassification Date – *Under Executive Order 12958, at the time of original classification, the Original Classification Authority must try to establish a specific date or event, not to exceed 10 years, when information may be declassified.*

Within CAPCO portion markings are included at the beginning of portions, such as paragraphs, to afford maximum visibility to the reader. Given that these markings reflect the sensitivity of the portion only, they may be less restrictive than the markings for a document as a whole.

3.19 French MOD Electronic Labelling Study

The French MOD Electronic Labelling Study started in September 2002 and finished at the end of 2003. It examined a number of technology products with labelling capabilities. It also proposed an XML Security Container (XSC), as seen in Figure 5, that was implemented in a java library and assorted applications.

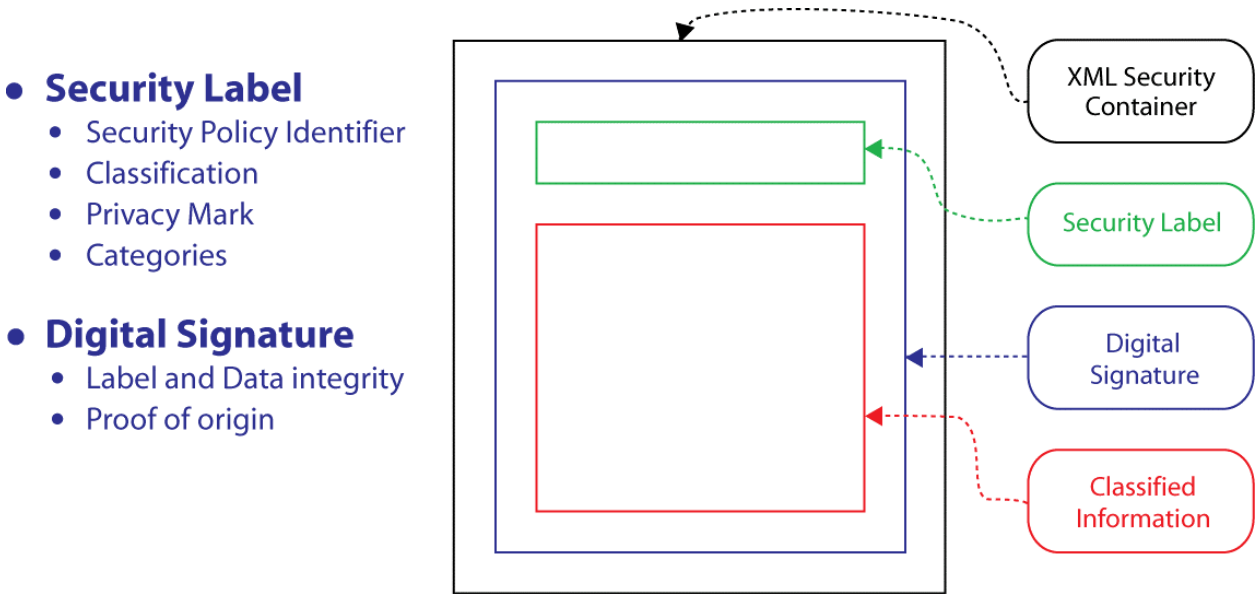


Figure 5 - XML Security Container³⁸

³⁸ Figure 2 is a re-production of a figure that appeared in French MOD Electronic Labelling Study [43].

3.20 Global Information Grid ³⁹

The GIG is a DoD project to ensure that U.S. and coalition forces have the information they require to conduct operations and as a result can achieve information superiority over their adversaries in a conflict. It is defined as *the globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services to achieve information superiority.*

Both the Intelligence Community (IC) and the Department of Defense (DoD) are developing metadata standards, and they are coordinating their work to ensure that IA attributes associated with RAAdAC style access control decision-making and discovery are addressed in these standards. However, standards development activities must be closely coordinated with ongoing research and development efforts, in order to avoid incompatibilities in technology standards that would eventually require changes to supporting tools, infrastructure, and large quantities of existing metadata records.

Annex A shows the minimum set of IA attributes needed to support policy based access control decision-making via the RAAdAC information-sharing model, based on the class of object.

3.20.1.1 Intelligence Community Markup Language ⁴⁰

IC Markup Language (ICML) was developed by the IC Metadata Sub-Working Group (MSWG) as part of the ICCIO Executive Council and Working Group commitment to IC inter-organization interoperability. Its purpose is to provide a common set of XML elements (TAGS) for implementing security-based metadata throughout the IC. It is designed around the CAPCO security markings specification and other related sources, capturing the security classification, control markings, and dissemination controls.

ICML is described as a Document Type Definition (DTD). The ICML DTD defines tags, much like HTML, that communicate important descriptive and structural information about intelligence content that resides within a document, product, or information module. ICML introduces: 1) various document/product structures, such as reports, articles, and analytical packets; 2) a new, expanded collection of document/product metadata broken into administrative and descriptive categories; 3) the most commonly used generic document components, such as paragraphs, lists, tables, and media; 4) CAPCO-compliant security models; and 5) descriptive content tags for more clearly indicating the subject matter of the information.

This release of the ICML is version 0.5. It is targeted for use by all intelligence production components of the nine agencies, the four military services, the J2, the nine unified commands, and the three national centers (counterterrorism, counterintelligence, and crime and narcotics).

³⁹ Net-Centric IA Strategy [44] and GIG IA Capability / Technology Roadmap [10] were used to provide content for this section of the report.

⁴⁰ IC MWG [45] was used to provide content for this section of the report.

It is expected that this release, and subsequent releases, will be commented on by any and all of these components as part of a continuing effort to develop and deploy standards that are applicable to the widest IC audience possible.

3.20.1.2 DoD Discovery Metadata Specification ⁴¹

The Department of Defense Discovery Metadata Specification (DDMS) defines discovery metadata elements for resources posted to community and organizational shared spaces. “Discovery” is the ability to locate data assets through a consistent and flexible search. The DDMS specifies a set of information fields that are to be used to describe any data or service asset that is made known to the Enterprise, and it serves as a reference for developers, architects, and engineers by laying a foundation for Discovery Services. The DDMS will be employed consistently across the Department’s disciplines, domains and data formats.

Security Set elements enable the description of security classification and related fields. These fields provide for the specification of security-related attributes and may be used to support access control. The security set is intended to support comprehensive resource security markings as prescribed by CAPCO. To accomplish this the DDMS refers to the IC ISM implementation of the CAPCO standards. For communities for which IC ISM does not suffice, additional security elements may be represented using the metadata elements defined by organizations and COIs, and stored in the Extensible Layer.

3.21 DND Metadata Application Profile ⁴²

The purpose of this Metadata Application Profile (MAP) is to fully describe specifically how to apply each of the DND core metadata elements and associated refinements to unstructured information resources. The following principles were followed when the MAP was created and shall be used when future additions to the elements or refinements are created:

- *It will be **Independent**. It will not be software, application or project based, but flexible enough to meet the information retrieval and records management needs, amongst others, of any information held in any format.*
- *It will be **Simple** to use. The standard must be readily applicable by those with widely varying experience of preparing information resource descriptions.*
- *It will be **Compliant with other GoC standards and policies**.*
- *It will be **Compliant with international standards**. Information is an international resource, and the DND/CF aims to remain a leader in the global information revolution. To achieve this, the metadata standard must reflect international standards and systems. If an international standard is appropriate and kept up to date it will be used. Preference will be given to standards with the broadest remit, so appropriate international standards will take preference over Allied standards, Allied standards will take preference over GoC standards.*

⁴¹ DoD DDMS [46] was used to provide content for this section of the report.

⁴² DND Metadata Application Profile [47] was used to provide the content for this section of the report.

- It will be **Stable**. Changes to a standard that will become embedded in all information systems will require considerable effort, time and resources to implement. MAPs must therefore be flexible enough to meet future as well as current needs.
- It will be **Extensible**. Additional element refinements can be added where it can be shown that these are essential and the existing set does not make provision for the requirement. A balance will need to be struck between the need for extensibility and the need for stability.
- It will be **Economical** by saving staff considerable time in searching for or retrieving information.
- It will be **Inclusive**, taking into account the many existing metadata schemes, with the aim of minimizing the need to rework existing products. This will be balanced with the need for maximum interoperability, which requires consistency across all information resource descriptions.
- Above all, it will **meet the information retrieval and management needs** of the department's users.

Annex B details the DND MAP securityMarking element, along with its attributes.

3.22 NC3A XSLS⁴³

The NATO C3 Agency (NC3A) XML Security Label and Processing specification defines an XML security label element type in order to represent the security classification or sensitivity of data. The intent is to assign security labels to digital data and provide automated access control based on these security labels.

NC3A built an experimental prototype, the XML Security Labelling System (XSLS), based on this specification. The prototype performs two main tasks. The first task is to assign security labels to files using XML security labels as defined in the XML Security Label and Processing specification. Labelling is done with an editor that assigns digitally signed labels to files. The second task of the XSLS system is to perform access control to the labelled files at the interconnection to an external system. This is done by a releasing gateway that mediates access to the labelled files.

- a. Producer – The producer consists of a custom developed security labelling editor responsible for performing labelling of files. The editor is a GUI Java application that allows the user to create a security label as defined in the XML Security Label and Processing specification. The security label is stored in a separate digitally signed XML file that includes a URI reference and hash of the file that the label applies to.
- b. Presenter – The presenter is a web server hosting the files and the associated XML security label files. The file and its associated XML label file are held in a common directory with a standardized file name for the XML label file.

⁴³ Alternative XML-Security Label Syntax and Processing [48] and XML Security Labeling System Prototype Architecture [49] were used to provide content for this section of the report.

- c. Releaser – The releaser is a Java HTTP proxy that intercepts the web traffic between the consumer and the presenter and checks that files are labelled appropriately before releasing them to the consumer. The proxy acts on consumer requests for files at the presenter by downloading the requested file and the associated XML label file from the presenter. It then proceeds by checking if the label value is either NATO UNCLASSIFIED or NATO RESTRICTED which are the classifications that can be released to the consumer. If the label value is appropriate for release, the proxy releases the file if the reference from the label file to the data file and the digital signature of the label file both are valid. If the label is not appropriate for release of the file or if the reference or digital signature validation fails, an error message is returned to the consumer.
- d. Consumer - The consumer is a web browser on a computer.

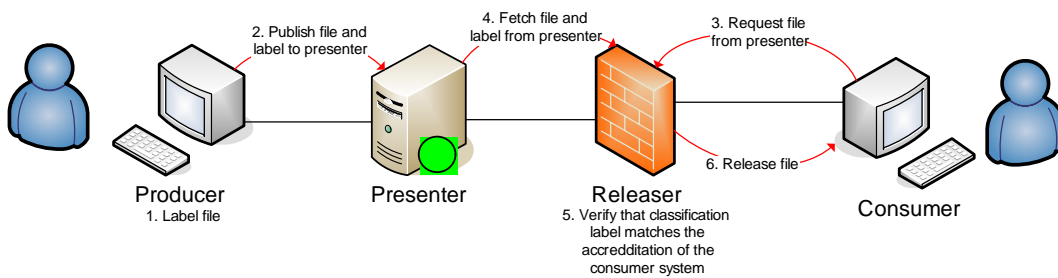


Figure 6 - XSL Security Labelling System Prototype Architecture ⁴⁴

⁴⁴ Figure 6 was taken from XML Security Labelling System Prototype Architecture [49].

This page intentionally left blank.

4. Commercial Approaches

4.1 Overview

Although there are exceptions, most notably databases, messaging systems and multilevel operating systems, security labels have not been incorporated into the majority of commercial products. In all likelihood, this is directly related to the market demand, or lack thereof, for this functionality. Historically, security labels have been considered an integral component of MLS products and their ability to enforce MAC. The challenges associated with developing, evaluating and deploying MLS solutions has likely detrimentally affected the inclusion of security labelling functionality in many products.

This section looks at how security labelling has been incorporated into a number of commercial products. While specific products containing security labelling functionality are listed in Annex C, the general categories of commercial products discussed in this section are as follows:

- Databases;
- Digital Rights Management;
- Document Management;
- Messaging;
- Multilevel Network; and
- Multilevel Operating System.

4.2 Databases

A number of commercial databases provide a security labelling capability as part of the application's access control system. Security labels are applied to objects within the database. When a user attempts to access a sensitive object, the subject's label (e.g., clearance) is compared against the label on the object. Provided the labels are equivalent, or that the subject's label dominates the object's label, access is granted to the object. Otherwise, access is denied.

The majority of these databases are capable of applying security labels to the table level. In many cases, more granularity is required than at the table level. Row level security allows data stored within tables to be further restricted. Row level security can either be provided through the use of views or by assigning security labels to individual rows in a table. A view can be used to limit the display to selected columns or a subset of rows from the base table. Unfortunately, the management of large numbers of views can be burdensome. The preferred option for row level security is the use of security labels, although this necessitates additional programming logic be embedded in the application.

4.3 Digital Rights Management

Digital Rights Management (DRM) is a means to control the use of digital content, even if the digital content has already been distributed. While the intent of DRM is not to provide a means to apply a security label to objects, it was proven that the publishing license that is included with objects as part of the publishing process can be used for just this purpose.

Within SAMPOC II, Microsoft Rights Management, based on eXtensible Rights Management Language (XrML) v.1.2.1, was used to protect information objects stored on a file server. Using pre-defined policy templates within Microsoft Office 2003 Professional, the application (Word, Excel, PowerPoint) created a unique XrML 1.2.1 publishing license for each object. The publishing license was then sent to the Windows Rights Management Server to be digitally signed, returned to the application and attached to the encrypted document. The Policy Enforcement Point (PEP), co-located with the file server, used the policy template name found in the publishing license as the security label. In order to enable the policy server to mediate access to the information object, the PEP sent the security label to the policy server.

Although XrML was specifically cited, there are a number of DRM initiatives to choose from, including the following:

- XrML - XrML *provides a universal method for securely specifying and managing rights and conditions associated with all kinds of resources including digital content as well as services.*⁴⁵ Although XrML originated at the Xerox Palo Alto Research Center (PARC) and is currently governed by ContentGuard Inc., it is most widely associated with Microsoft's DRM solutions.
- Open Digital Rights Management (ODRL) Initiative – The ODRL initiative *is an international effort aimed at developing and promoting an open standard for the Digital Rights Management expression language.*⁴⁶
- Open Media Commons – Open Media Commons originated within Sun Microsystems Laboratories as a project (Project DReaM) to develop an open, end-to-end content-protection solution.

4.4 Messaging

Commercial messaging systems typically provide confidentiality, integrity and non-repudiation services but rarely provide a security labelling capability. Those that do provide this capability tend to include human readable security markings in both the subject line and the message body, in addition to the electronic security labelling information. While the security label can be used to enforce access control, the security markings are used to promote user awareness. There is currently no standard for Messaging Application Programming Interface (MAPI) and Simple Mail Transfer Protocol (SMTP) security labels. The S/MIME security label standard was discussed in some detail in Section 3.17.

⁴⁵ XrML [50]

⁴⁶ ODRL [51]

In addition to basic security labelling functionality, some messaging systems allow security officers to customize the security policies that govern security labelling. This customization includes defining levels of classification and caveats, specifying default security labels and enforcing whether or not security labels must be included with each message sent. Some messaging systems even allow security labels to be linked with enforceable DRM policies.

4.5 Multilevel Network

A multilevel network, sometimes referred to as a labelled network, *is one where a single network is used to communicate data with different sensitivity information (e.g., Unclassified, Company Proprietary, Secret).*⁴⁷

There are two approaches to multilevel networking. The first approach relies on cryptography to provide the necessary level of separation and prevent leakage of classified information through malicious interception or inadvertent delivery. This implicit approach does not include security label information with each packet. Rather, it relies on another attribute (i.e., cryptographic key) to determine the security label. In this scenario, multilevel network interfaces (e.g., bridges, firewalls, gateways, routers) need to be capable of interpreting this implicit approach to security labelling. Using this approach, hosts would only be capable of decrypting network packets at a certain level.

The second, and preferred, approach inserts security labels in the network packets and relies on a reference monitor mechanism within multilevel network interfaces to enforce security policy. This explicit approach includes security label information in each packet, as part of the Protocol Control Information (PCI). Using this approach, hosts would only receive network packets with the appropriate security label.

*MLS networks can interconnect single-level and multilevel components on a shared network infrastructure by providing sensitivity labels and network security services for the data transferred between systems. MLS networks do not need to have any MLS hosts or workstations on them to make them effective solutions; the MLS networks may simply allow single-level hosts and workstations of different security levels to share a common infrastructure.*⁴⁸

4.6 Multilevel Operating Systems

*Existing mainstream operating systems lack the critical security feature required for enforcing separation: mandatory access control. As a consequence, application security mechanisms are vulnerable to tampering and bypass, and malicious or flawed applications can easily cause failures in system security.*⁴⁹

Multilevel operating systems incorporate a number of capabilities that attempt to limit the potential harm caused by these malicious or flawed applications. Furthermore, multilevel

⁴⁷ Trusted Network Interpretation of the TCSEC [52]

⁴⁸ Multilevel Security in the Department of Defense: The Basics [53]

⁴⁹ SELinux [54]

operating systems allow information with different sensitivities to be stored and processed on the system, while enabling and mediating access by users with varying security clearances. Security labels are an integral component in providing this capability. Multilevel operating systems apply security labels to all data objects and information flows, including networks, packets, files, directories, devices, windows, memory, processes, and interprocess communication mechanisms. Devices include frame buffers, tape drives, diskette and CD-ROM drives, serial ports, network interfaces and USB ports. Security labels are used by the MAC within the operating system to enforce the Bell-LaPadula security policy. In addition to security labels, human readable security marking information is sometimes used to label windows and included on printer banner and trailer pages.

5. Requirements

5.1 Overview

This section will attempt to develop a number of requirements that can be used in the development/procurement of a security labelling capability for DND, and specifically for SAMSON. The requirements being developed are in the following areas:

- Object & Application Support;
- Structure;
- Syntax;
- Trust & Assurance; and
- General.

5.2 Object & Application Support

The format of electronic labels will differ somewhat depending on the types of data transmitted or stored, and the protocols used to transmit them. For example, electronic mail messages tend to be represented in one of a few character encoding formats, using well established protocols, and are expected to be both stored and transmitted en route from a single sender to a single receiver. By contrast, streaming multimedia is often in proprietary format, using evolving protocols, and is expected to be ephemeral, with extended transmission time, and may be broadcast. In the latter case, it is also usual to capture a segment of the data, and store it. Clearly, a label appropriate for messages is not suitable for streaming multimedia. Further, a label defined now for a well-understood transmission mechanism (such as messaging) will very likely not work for an area of information transmission that is still evolving (such as streaming multimedia).⁵⁰

This section will examine object and application support requirements in the following areas:

- Object Classes;
- Legacy Support; and
- SAMSON Applications.

5.2.1 Object Classes

Section 2.2 defined a number of object classes likely to exist within the DND operational environment. The security labelling capability will eventually be required to support each of these object classes. Furthermore, the label format, as well as the syntax and binding mechanism may need to be adapted for different object classes.

⁵⁰ Electronic Labelling of NATO Information [39]

Requirement #1 – The security labelling capability must support the object classes required for the DND operational environment. These include the following object classes: information objects, service objects, session objects and real-time objects.

5.2.2 Legacy Support

In most large organizations there currently exists a large number of legacy information and service objects. These legacy objects, traditionally stored in system high environments, either have no security label or in limited cases, a proprietary security label. This legacy information will need to incorporate the new security label in order to facilitate information access and sharing.

Given the vast quantities of legacy information, it would be a time consuming task to attempt to classify each information object individually and apply the corresponding security label. An automated capability is required to scan the content of the information object and based on a number of rules, assign the correct security label to the information object.

Requirement #2 – The security labelling capability must support an automated labelling capability whereby legacy information stored on servers can be appropriately labelled without human involvement.

5.2.3 SAMSON Applications

Five initial applications have been identified by the SAMSON Stakeholders Working Group. The security labelling capability must be able to support each of these applications. The five applications are as follows:

- Chat;
- Database;
- Documents (Microsoft Office suite of applications);
- Email; and
- Web Content.

Requirement #3 - The security labelling capability must support the following SAMSON applications: chat, database, documents, email and web content.

5.3 Structure

This section will examine requirements related to the structure of the security label, specifically in the following areas:

- Data Format;

- Labelling Approaches;
- XML-based Security Label and Digital Signature Type.

5.3.1 Data Format

eXtensible Markup Language (XML) is a specification developed by the W3C. XML is a subset of SGML, designed especially for Web documents. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.⁵¹

There are a number of benefits to using XML that are equally applicable to the use of XML as the data format for security labels. The benefits are as follows:

- *Simplicity - Information coded in XML is easy to read and understand, plus it can be processed easily by computers.*
- *Openness - XML is a W3C standard, endorsed by software industry market leaders.*
- *Extensibility - There is no fixed set of tags. New tags can be created as they are needed.*⁵²

Requirement #4 - The security labelling capability must support XML-based labels in order to facilitate extensibility and interoperability.

5.3.2 Labelling Approaches

While both implicit and explicit approaches to security labelling are valid, there are a number of advantages to using explicit labelling to facilitate caveat separation. Explicit security labelling facilitates access mediation and minimizes confusion by explicitly providing security labelling information for each object.

Requirement #5 - The security labelling capability must use explicit labelling in order to minimize confusion and facilitate access mediation.

⁵¹ Webopedia [17]

⁵² XML [55]

5.3.3 XML-based Security Label and Digital Signature Type

The main lesson learned (from the NC3A XLSL prototype – refer to Section 3.22) is that it could be beneficial to decouple the XML security label and the XML signature. Detached labels are still enabled by referencing both the security label and the labeled object with references inside an XML digital signature. This decoupling has the benefit of enabling standard XML digital signature validation to include the validation of the XML security labels. The main disadvantage of this construct is that it obscures the link between label and labeled object by hiding it in the references of a digital signature and that it in some complex scenarios of multiple labels applied to multiple objects requires multiple digital signatures.⁵³

The notable exception to this rule is the case of XML-based objects where partial security labelling is required. XML-based documents with paragraph level security labels are a good example of this.

Requirement #6 - The security labelling capability must use a detached security label and digital signature for objects that are not XML-based. Decoupling the security label and digital signature will facilitate validation of the security label.

Requirement #7 – The security labelling capability must use either an enveloped or enveloping security label and digital signature when the object is XML-based. This will allow security labels to be applied and bound to a portion of the object.

5.4 Syntax

In order for security labels to prove useful as part of a caveat separation solution they must include a number of attributes to facilitate access mediation. Attributes that need to be included in the security label are as follows:

- Classification;
- Caveat;
- Foreign Classification;
- Security Policy;
- Access Rights;
- Expiration; and
- Quality of Protection.

⁵³ Alternative XML-Security Label Syntax and Processing [48]

5.4.1 Classification

Levels of classification were discussed in some detail in Section 2.3.1. The classification attribute is equivalent to Security Classification in the S/MIME Security Label, Classification in CAPCO, Sensitivity Level in the GIG IA attributes and Classification in the DND MAP.

Requirement #8 – The security label must specify the level of classification of the object. This attribute is mandatory for all objects.

5.4.2 Caveat

Caveats were discussed in some detail in Section 2.3.3. The caveats attribute encompasses aspects of Security Categories in the S/MIME Security Label, SCI Control System Markings and Dissemination Controls in CAPCO, Releasability in the GIG IA attributes and Control System, Dissemination Control and Releasable To in the DND MAP.

Requirement #9 – The security label must specify the caveats associated with the object. This attribute is mandatory for all objects.

5.4.3 Foreign Sensitivity

Foreign sensitivity is intended to represent the classification and applicable caveats for objects originating outside of Canada. The foreign sensitivity attribute encompasses aspects of Equivalent Security Labels in the S/MIME Security Label, Non-US Classification Markings, Foreign Government Information and Non-Intelligence Community Markings in CAPCO, Foreign Classification, Contains Foreign Information and Non Intel Community in the DND MAP.

Requirement #10 – The security label must specify the foreign sensitivity of the object. This attribute is mandatory for all objects originating outside of Canada.

5.4.4 Security Policy

The primary requirement for a security label is for enforcing mandatory access control over sensitive objects according to a central security policy. The security label will contain the information required by the policy framework to mediate access, provide content-based encryption and enforce proper handling. In the case of access mediation, the security label will either directly or indirectly reference the security policy that will ultimately be used to mediate access to the sensitive object. In the direct case, the security label will reference the security policy specifically. In the indirect case, attributes of the security label will be used to determine the applicable security policy.

The security label attribute is equivalent to Security Policy Identifier in the S/MIME Security Level and Security Policy Index in the GIG IA attributes.

Requirement #11 – The security label must support, either directly or indirectly, policy-based mediation. This attribute is optional for all objects.

5.4.5 Access Rights

Access rights specify acceptable actions that can be performed on the object by authorized users. The access rights attribute encompasses aspects of Access Control Information List/Policy in the GIG IA attributes and Access Rights in the Rights element of the DND MAP.

Requirement #12 – The security label must specify the access rights associated with the object. This attribute is mandatory for all objects.

5.4.6 Expiration

Expiration specifies the date in time after which no further access to the object is permitted. The expiration attribute is equivalent to Time to Live in the GIG IA attributes.

Requirement #13 – The security label should specify the expiration date associated with the object. This attribute is optional for all objects.

5.4.7 Quality of Protection

There are three basic security services applied to protect information from which all other services, mechanisms and products can be derived. They are:

- a. Confidentiality - Protection of information from unauthorized disclosure;*
- b. Integrity - Protection of information from unauthorized modification and destruction;
and*
- c. Availability - Protection of information systems from unauthorized denial of service.⁵⁴*

Security labels can be used as the basis for a data-centric model, in which information is protected according to its content. The security label can indicate additional requirements for confidentiality, integrity and availability. For example, the security label could specify that the

⁵⁴ DND Information Security Technology Security Architecture [56]

object be encrypted with AES or that it should only be sent over a specific network path, thus ensuring its availability.

Requirement #14 – The security label should specify the quality of protection associated with the object. This attribute is optional for all objects.

5.5 Trust & Assurance

In order for a security label to serve as a critical component of the access mediation process in a caveat separation solution, the mechanism binding the security label to the object must be trusted and the labelling solution must be evaluated, certified and accredited. This section examines these two issues.

5.5.1 Binding Mechanism

Security labels must be linked to the objects in a trusted manner to prevent unauthorized changes. Failure to include a trusted binding mechanism will enable those with malicious intent to alter, replace or remove security labels without detection. Two potential alternatives for binding security labels with objects have been identified:

- Digital Signature - *One method to associate labels with data is to use a digital signature. The signature enables detection of any modification to the data object or security label, and signals the intent of the signer to have the label associated with the data object. (The data object may itself be signed; this provides separate integrity of the data object but does not cryptographically bind the label to the data object).*⁵⁵ There are two relevant standards for digital signatures. They are as follows:
 - Cryptographic Message Syntax (IETF RFC 2630)
 - OASIS XML-Signature
- Database - *Alternatively, the information storage server can provide an association between a label and its data object. For instance, an information server may store both the information and the label as separate data objects. The server would be responsible for ensuring that labels were processed as part of information access, and that the correct label is processed.*⁵⁶

Requirement #15 – The security labelling capability must bind security labels to objects in a trusted manner in order to prevent unauthorized changes.

⁵⁵ Electronic Labelling of NATO Information [39]

⁵⁶ Electronic Labelling of NATO Information [39]

5.5.2 Evaluation, Certification & Accreditation

There are two aspects of security products that must be addressed before a product can be authorized for implementation:

- a. Functionality - Verification that the product does what it is supposed to do; and*
- b. Assurance - Verification that the product does what it is supposed to correctly, and that it does not do anything else.*

Of these two, assurance is by far the hardest to prove, as it can demand a great breadth and depth of activity from formal mathematical modeling to comprehensive testing.⁵⁷ Assurance, which is defined as the degree of confidence that a product correctly implements the security policy⁵⁸, is the result of a rigorous process that includes the following steps:

- 1. Evaluation – The process of achieving assurance given a security policy, a consistent description of the security functions and a targeted assurance level.*
- 2. Certification – The comprehensive assessment of the technical and non-technical security features of an information technology system, made in support of accreditation, that establishes the extent to which a system satisfies a specified security policy.*
- 3. Accreditation – The authorization that is granted for the use of an information technology system to process information in its operational environment.⁵⁹*

Given the lack of products in this area it may not be realistic at this time to stipulate that only evaluated products be used.

Requirement #16 – The security labelling capability must be capable of undergoing formal evaluation as part of the evaluation, certification and accreditation process.

5.6 General

This section is a catchall for requirements not covered by the previous sections. It addresses the following areas:

- Awareness;
- COTS;
- Interoperability; and
- Translation.

⁵⁷ DND Information Security Technology Security Architecture [56]

⁵⁸ CTCPEC [19]

⁵⁹ CTCPEC [19]

5.6.1 Awareness

While electronic security labels facilitate policy enforcement and in this particular case, caveat separation, they must also promote user awareness. Only by prominently displaying security label information in a human-readable form can we increase user awareness and increase the likelihood of sensitive objects being properly handled.

Requirement #17 – The security labelling capability must promote user awareness and consequently proper handling through human-readable security markings.

5.6.2 COTS

*Commercial-off-the-shelf (COTS) products are to be used to the maximum extent possible. Development is expensive, risky, and in the rapidly changing IT market, usually unsupportable. In addition, the commercial products used must support open standards wherever possible.*⁶⁰ Security labelling solutions should be no exception to this general principle.

Requirement #18 – The security labelling capability must leverage COTS products to the maximum extent possible.

5.6.3 Interoperability

Given DND's requirement for collaboration with other government departments, coalition partners and allies, security labels must be presented in a standardized manner to facilitate information sharing. Interoperability is complicated by the lack of a pervasive security labelling standard. The end result being that different countries, and in many cases different departments and agencies within the same country, will apply different security labels to objects.

Interoperability cannot be achieved unless a standardized security label can be agreed upon. This standardized security label must have a well defined syntax that specifies both mandatory and optional elements and attributes. Furthermore, the semantics must be agreed upon as well in order to prevent misinterpretation. For example, although two countries may label an object Confidential, the term may have completely different security requirements in the two countries.

Requirement #19 – The security labelling capability must facilitate eventual interoperability with other government departments and allies through the use of an extensible labelling syntax.

⁶⁰ DND Information Security Technology Security Architecture [56]

5.6.4 Translation

Security label translations should be avoided whenever possible by using a security label format that is supported by all systems that will process the security label.

Requirement #20 – The security labelling capability must avoid security label translations by using a standard format supported by all systems.

6. SAMSON Security Labelling

6.1 Overview

The SAMSON security labelling strategy is to define an XML-based security label and ensure that it is bound/linked to SAMSON objects in a trustworthy manner. Security labelling plug-ins and server components will be included as required in order to support the SAMSON applications as identified by the SAMSON Working Group. This section will address the following aspects of the SAMSON security labelling component:

- Approach;
- Strategy;
- Level of Effort; and
- Cost Estimate.

6.2 Approach

Although there are a number of proposals for an XML-based security label, there is no consensus. Furthermore, none of the labelling proposals satisfies all of the requirements for the SAMSON environment. For these reasons, SAMSON will utilize an XML-based security label sufficient for its own purposes but flexible enough to leverage emerging standards as required. This XML-based security label will be sufficiently flexible to enable it to be used for documents, web content and potentially chat. In all likelihood, the database will leverage the security labelling functionality of a commercial database, while the email will leverage the S/MIME Security Labelling standard. Figure 7 illustrates the recommended security labelling approach for the SAMSON applications.

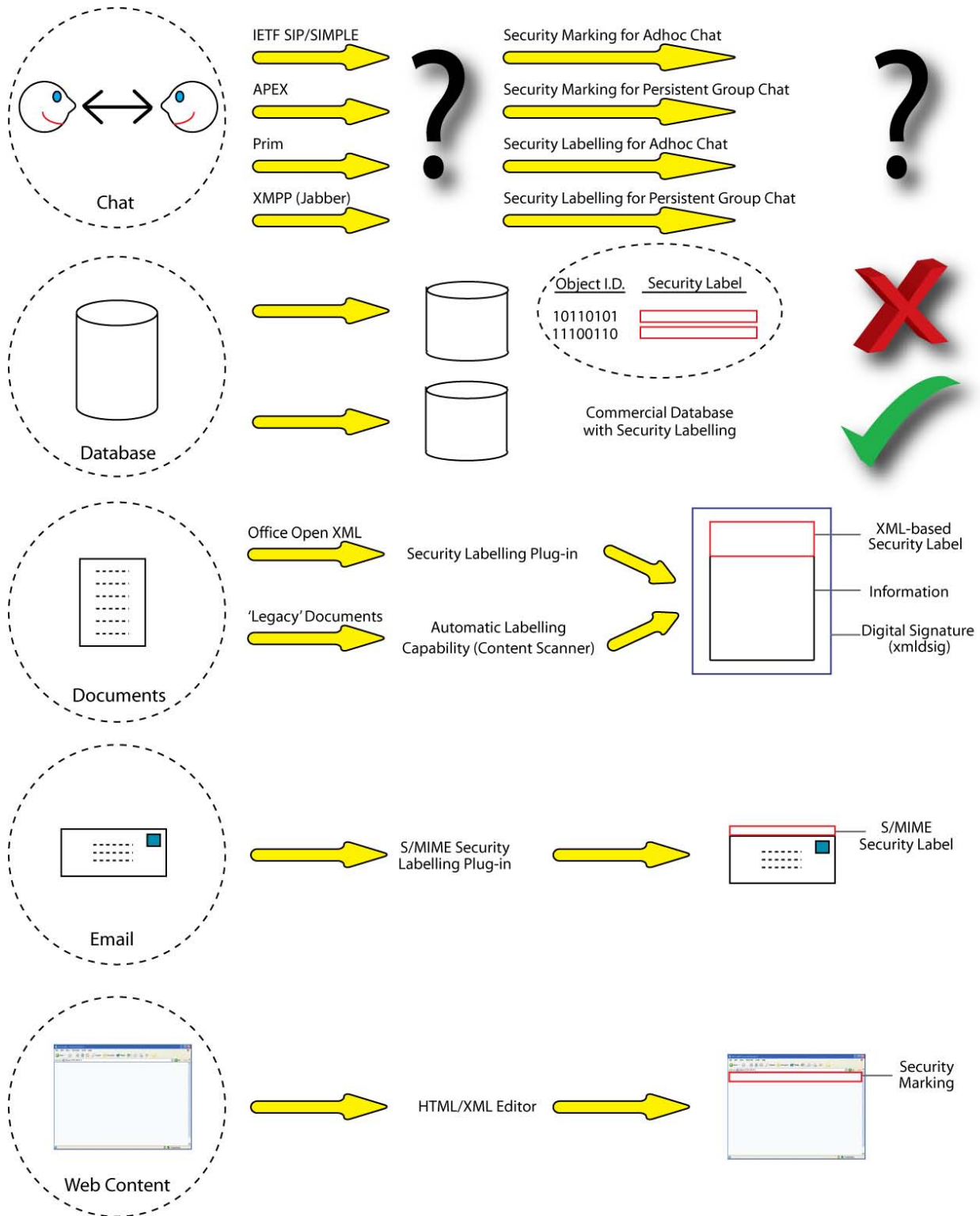


Figure 7 - SAMSON Security Labelling Approach

6.2.1 Chat

Instant Messaging (IM), also referred to as chat, is *a type of communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet, analagous to a telephone conversation but using text-based, not voice-based, communication. Typically, the instant messaging system alerts you whenever somebody on your private list is online. You can then initiate a chat session with that particular individual.*⁶¹

Chat is used extensively over the Internet through public IM services such as America On Line (AOL), MicroSoft Network (MSN) and Yahoo. In the classified environment there would be no connection to these public IM services. Rather, DND would host an enterprise IM service that would provide a chat capability throughout the enterprise domain. Such a service would enable users to detect another user's availability. This functionality, known as presence awareness, enables users to display their status (e.g., away, idle, busy, do not disturb) to other users. This in effect allows users to control which users can see their presence and consequently which users can communicate with them.

It is next to impossible to fully develop an approach to applying security labels to chat sessions as a result of the number of unknowns with respect to DND's use of IM technology in the classified environment. For example, it is currently unclear what enterprise chat server, if any, DND intends to standardize on. Given that many IM systems use different technologies, that each leverages a competing instant messaging protocol, it is currently impossible to develop a specific approach to security labelling for chat. A number of the more popular instant messaging protocols include the IETF's SIP (Session Initiation Protocol) and SIMPLE (SIP for Instant Messaging and Presence Leverage), APEX (Application Exchange), Prim (Presence and Instant Messaging Protocol), and the open XML-based XMPP (Extensible Messaging and Presence Protocol), more commonly known as Jabber.

Furthermore, it is currently unclear whether this technology is required for adhoc chat, for persistent group chat or for both. Adhoc chat, or IM, enables users to use the presence detection to determine if a particular user is online and initiate a private chat session with that person. Additional users can be invited to join this adhoc chat session as required. Persistent group chat is basically a chat forum that is constantly up and running. Provided a user has membership to the particular group, the user will be able to join the chat session at any time. Furthermore, the persistent group chat maintains a message history for ongoing communications that can be examined and searched by users.

In all likelihood, DND will require both an adhoc chat capability and a persistent group chat capability. Assuming that this is the case, there are four distinct methods with which to appropriately label chat sessions. Further discussion with stakeholders will be required to determine the preferred method(s). The methods are as follows:

- Security Marking for Adhoc Chat – Security markings are a critical requirement for adhoc chat sessions. Although security markings do nothing to enforce policy, they serve to promote user awareness and encourage discretionary enforcement. The security marking, which would be displayed prominently at the top of the chat window, would represent the highest level of discussion that could take place in a given chat session. Furthermore, the

⁶¹ Webopedia [17]

security marking would need to be dynamic in order to reflect the changing membership in a particular chat session. For example, Captain Alice notices that a colleague, Captain Bob, is on-line. She immediately initiates a chat session with Captain Bob in order to discuss relevant issues. Since both participants are Canadian citizens who are cleared to Secret, the client-side plug-in would prominently display the security marking 'Secret CEO'. This security marking reflects the highest level of communication possible in the current chat session. During the chat session between Captain Alice and Captain Bob an issue comes up that can only be resolved by a third-party, Captain Washington. Seeing that Captain Washington is on-line, Captain Alice invites him to join the current chat session. Since Captain Washington is a U.S. citizen who is cleared to Secret, the security marking would need to change to 'Secret CANUS' to reflect the current membership of the chat session.⁶²

- **Security Marking for Persistent Group Chat** – In all likelihood, it will be easier to apply security markings to a persistent group chat session than to adhoc chat. The reason is that the persistent group chat security marking is a static value, set when the forum is established, that does not change to reflect its participants. For example, Captain Alice, a Canadian duty shift officer, relieves Captain Bob after a particularly gruelling shift. After a brief turnover Captain Alice joins the Secret CEO persistent group chat session. She can now review the message history in order to determine what has transpired while she was off shift. Captain Alice's access to the Secret CEO forum is determined by Access Control Lists (ACLs) maintained by the application.
- **Security Labelling for Adhoc Chat** – In this scenario, the participant initiating the chat session does so at a certain level (e.g., Secret CEO). A policy enforcement component would ensure, based on the chat security label, that all potential participants were cleared to participate in a particular chat session. For example, Captain Alice notices that Captain Bob is on-line. Since she would like to discuss a potentially sensitive issue with him, she initiates the chat session at the level 'Secret CEO'. Before the chat session is initiated with Captain Bob, the policy enforcement component ensures that Captain Bob is cleared to participate in a chat session at that level. As with security marking for adhoc chat, the security marking would be displayed prominently at the top of the chat window. During the chat session between Captain Alice and Captain Bob an issue comes up that can only be resolved by a third-party, Captain Washington. Seeing that Captain Washington is on-line, Captain Alice invites him to join the current chat session. Prior to Captain Washington receiving the invitation to join this particular chat session, the policy enforcement component determines whether or not Captain Washington is cleared to do so. In this particular case, he is not cleared and Captain Alice is notified accordingly. In order to include Captain Washington in subsequent discussions, Captain Alice must initiate a new chat session at the Secret CANUS level.
- **Security Labelling for Persistent Group Chat** – There is a subtle difference between security labelling for persistent group chat and security marking for persistent group chat. While the latter relies on the application, through ACLs, to determine whether or not a user can participate in a forum, security labelling for persistent group chat actually assigns the appropriate security label to the forum. This security label is used by the policy enforcement function in determining whether or not a particular user can join the forum. For example, Captain Alice, a Canadian duty shift officer, relieves Captain Bob after a particularly

⁶² Depending on the chat product used, it may be possible for new participants to view previous chat content. Either procedural or technical controls would need to be put in place in order to prevent unauthorized users from accessing previous chat content.

grueling shift. After a brief turnover Captain Alice attempts to join the Secret CEO persistent group chat session. The policy enforcement component, using the chat security label, determines whether or not Captain Alice is cleared to do so. Captain Alice is allowed to join the forum and is now able to review the message history in order to determine what has transpired while she was off shift.

- Automatic Enforcement for Adhoc and Persistent Group Chat – Through the use of a content scanner, both adhoc and persistent group chat sessions can be scanned in near real-time in order to ensure that the security label accurately reflects the dialog taking place. In cases where the dialog is determined to be more sensitive than the security label indicates, a number of actions could take place. These actions could range from a security officer being notified, to a warning being displayed to the chat participants, to the chat session being terminated.

Depending on DND's specific requirements and the product used, the security marking and labelling capabilities discussed in this section will likely necessitate a customized IM client as well as a policy enforcement component co-located with the enterprise chat server. The automatic enforcement capability would necessitate an automatic labelling capability. This is discussed in detail in Section 6.2.3.

6.2.2 Database

There are two approaches to consider when contemplating how to implement security labelling in a database. The first approach is to link an XML-based security label to a particular object and store it in either an XML-enabled or native XML database. This approach will necessitate the development of a security labelling administrative console capable of creating XML-based security labels, linking them to the appropriate object and storing them in the database. It will also necessitate the development of PEPs capable of retrieving, validating and parsing these XML-based security labels.

The second, and preferred, approach is to leverage the labelling capability built into some commercial databases. This was the approach adopted for SAMPOC II. The advantage of this approach is that it enables the security labels to be administered from an existing administrative interface. However, it does necessitate the development of PEPs capable of retrieving, validating and parsing these proprietary security labels. In addition to being the preferred approach from an ease of development perspective, commercial databases are likely to have been evaluated against the Common Criteria. In the case of proprietary database labelling mechanisms, the lack of evaluation may complicate the certification and accreditation process, ultimately delaying its approval for use within the DND classified environment.

6.2.3 Documents

SAMSON will eventually support Microsoft's upcoming Office Open XML formats for Word, Excel and PowerPoint documents. This XML-based format for documents will facilitate the exchange of information between Office documents and other enterprise applications. It will also

facilitate trusted labelling by including support for mapping customer-defined schemas into the content of Word and Excel files. Although the Open XML schema does not currently include elements containing attributes for security-related metadata, the schema can likely be extended to include such attributes. A Security Labelling Plug-in for Office Open XML would allow users to assign security labels to not only the entire document but to portions of the document as well. Furthermore, when a security label is assigned to the document as a whole, this would automatically apply the appropriate DRM template. Rights management effectively encrypts the zip container that holds all of the XML content.

In addition to this new Office Open XML format, SAMSON must be capable of supporting 'legacy' formats such as Adobe documents and traditional Office documents, as well as images, video files, etc. Much of this 'legacy' information is stored without standardized security labels on servers throughout DND. It is for this reason that an automatic labelling capability is an absolute requirement. The automatic labelling capability would consist of the following four components:

- Converter – Objects come in a variety of file formats. The converter accepts a wide variety of file formats and converts them into XML so that they can be content scanned.
- Content Scanner – The content scanner uses a combination of explicit rules and machine learning to scan XML in order to determine the appropriate security label. In the case of explicit rules, you know what you are looking for and you encode rules to automatically perform the search. For example, some legacy information may contain security labels at the paragraph level in a certain format. An explicit rule can be coded to search for these paragraph-level security labels. In the case of machine learning, the content scanner would be provided with a number of examples of appropriately labelled documents. Based on words and their co-occurrence the content scanner would be able to computationally determine appropriate security labels for new objects.
- Security Labeller – Once the content scanner determines an appropriate security label for a given object, the security labeller would generate an XML-based security label and cryptographically bind it to the original (not converted XML) object.
- Content-based Encryptor – Based on the security label of the object, the content-based encryptor would automatically generate a symmetric key and use it to encrypt the object. The symmetric key would in turn be encrypted by a central server's public encryption key.

6.2.4 Email

Not only is S/MIME the only email standard equipped to include security label information, but digitally signing the email message provides a means to bind the security label information to the body of the email cryptographically. It is for these reasons that S/MIME is the preferred approach to email security labelling within SAMSON.

6.2.5 Web Content

Web content, by its very nature, is amongst the easiest to apply a security label to. Given that web content is in either HTML or XML, any HTML/XML editor can be used to include the appropriate security labelling and marking information. The security label would take the form of the standard XML-based security label, with an XML digital signature used to provide the cryptographic binding. The web content would also include a security marking such that the security label was prominently displayed when viewed on a user's browser.

6.3 Strategy

Section 6.2 highlighted an approach to providing security labelling for SAMSON based on the requirements identified in Section 5. This section takes the approach one step further by identifying potential technologies that can be used to provide the SAMSON security labelling capability. It also identifies any shortcomings with these products and proposes a strategy to rectify them.

6.3.1 Chat

Due to the sheer number of unknowns in terms of DND's chat requirements, as detailed in Section 6.2.1, it is impossible to devise a specific strategy for the application of security labels to chat sessions for the classified environment. The recommended course of action is to interview SAMSON stakeholders in order to determine their specific requirements and develop an appropriate strategy that meets these requirements.

An alternate strategy, intended to demonstrate a capability only, would be to select an enterprise IM platform and client and proceed with the approach outlined in Section 6.2.1. For example, Microsoft Live Communications Server could be used along with a customized Microsoft Messenger Client to demonstrate a subset of the functionality outlined in Section 6.2.1.

6.3.2 Database

Given that Oracle is the de-facto standard database within DND and that Oracle Label Security provides most of the needed functionality, it would seem to be a logical choice. Furthermore, this combination proved successful in providing a security labelling capability for SAMPOC II.

Label-based access control provided by Oracle9i Label Security allows organizations to assign sensitivity labels to information, control access to that data based on those labels, and ensure that data is marked with the appropriate sensitivity label.⁶³ Oracle9i Label Security provides multi-dimensional, flexible data labelling capabilities. Oracle9i Label Security labels can include the following components:

⁶³ Oracle Database Security [58]

- **Level** – a hierarchical component which denotes the sensitivity of the data. A typical government organization might define levels confidential, sensitive and highly sensitive. However, there is no requirement to define more than one level. For example, a commercial organization might define a single level for company confidential data or application hosting requirements.
- **Compartment** – a component, sometimes referred to as a category, that is non hierarchical. For example, a compartment might be defined for an ongoing strategic initiative or map to a hosted application subscriber. Oracle9i Label Security supports up to 9999 unique compartments.
- **Group** – a component used to record ownership, that can be used hierarchically. For example, two groups called Senior VP and Manager could be created and subsequently assigned as children of the CEO group, creating an ownership tree.⁶⁴
- **Releasability** – Release 2 of Oracle9i Label Security supports releasabilities, adding even more flexibility to the Oracle9i Label Security access control capabilities. Releasabilities have historically been used in government organizations to control the dissemination of data. Releasing data to the entire marketing organization becomes as simple as adding the marketing releasability to the data record.⁶⁵

6.3.3 Documents

Titus-Labs has developed a security labelling plug-in for Microsoft Word aptly named Document Classification for Microsoft Word. This plug-in includes security labelling information in custom properties that are associated with the document. While these custom properties are currently customizable, they are finite. In order to extend them further currently requires the use of a sample macro. This product has a similar look and feel to, and much of the same functionality as, Titus-Labs' MessageRights product, discussed in Section 6.3.4. Furthermore, Document Classification for Microsoft Word integrates with Microsoft Rights Management. By associating a security label with the document, a DRM template is automatically assigned to the document, thus restricting its handling. In addition to Document Classification for Microsoft Word, Titus-Labs is investigating the possibility of providing similar plug-ins for both Excel and PowerPoint. Furthermore, it is Titus-Labs intention to port the current version to Office 12 when it is made available.

From a DRDC perspective there are currently two things missing from Document Classification for Microsoft Word. As a result, these two features will likely be missing from the Excel and PowerPoint versions, as well as any future Office versions. The two features are a standardized XML-based security label and a trusted binding mechanism. While the security label can be somewhat customized, it is not XML-based. Further investigation will be needed to determine whether the customization is sufficient. Furthermore, DRDC is advised to pursue a solution with Titus-Labs involving an XML-based security label, consistent with the DRDC schema, for Office 12. There are two solutions to the lack of a trusted binding mechanism. The first solution is to leverage the digital signature capability in Microsoft Word. The second solution is to include a

⁶⁴ Oracle Database Security [58]

⁶⁵ Oracle Label Security [59]

key that would be hidden in the software DLL. This key would be used by the plug-in to produce a hash of the word document, including custom properties. The plug-in at the receiving end would verify the hash using the same hard-coded key in order to ensure that the labels and the message had not been tampered with. The digital signature approach is the preferred option.

The automatic labelling capability could be provided by using a combination of the Entrust Entelligence Content Analysis Toolkit and re-using components of the Entrust Entelligence Compliance Server. The converter that is used as part of the Entrust solution is actually a product from Verity (www.verity.com) and sufficient for our purposes. The main part of the solution, the content scanner, is the core component of the Entrust Entelligence Compliance Server. However, explicit rules would need to be developed, and sample documents provided, in order to enable the content scanner to effectively classify SAMSON documents. Furthermore, both the security labeller and the content-based encryptor would need to be developed. Given Entrust's extensive background in digital signatures and encryption, neither of these components should prove overly onerous.

6.3.4 Email

Titus-Labs has developed a security labelling plug-in for Microsoft Outlook called MessageRights. It is basically their Message Classification product with Microsoft RMS integration built-in.

Titus Labs Message Classification has several features specifically tailored to the military environment:

- *users can be forced to make a selection - administrators can customize the software to force users to make a classification selection. Users will not be allowed to send mail until a classification has been assigned to the message*
- *on a Reply/Forward, downgrading of classifications can be prevented. - Administrators can customize the software so that users will not be allowed to downgrade classifications when Replying or Forwarding a message with pre-existing classification. This option can also be switched from Prevent to Warn. In the Warn mode, users will be allowed to downgrade a classification on Reply or Forward, but they will receive a warning message alerting them to possible consequences.*
- *For users of the US Defense Messaging System (DMS), the software can be set to insert a classification label on the first line of the message with or without a classification prefix. The Message Classification software can also append the label(s) as the last line of a message.*
- *Classification label can be inserted in the subject line of the message.*
- *can generate policy based disclaimers or signatures at the end of email messages based on a classification. For example if the "Confidential" label was selected the Message Classification software could automatically insert disclaimer text such as: "The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this*

information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer."

Titus Labs MessageRights provides all of the features of Message Classification and in addition provides the following features:

- *labels can be inserted to classify attachments, declassification dates and reason codes.*
- *only the appropriate labels are made available to the user based on their clearance - the user's clearance information, classification levels and project clearance information can be stored in Microsoft Active Directory where. MessageRights will dynamically build the available label for every user based on their rights. Users cannot classify above their clearance.*
- *users cannot send messages to recipients who do not have the clearances associated with the email - MessageRights powerful whitelisting feature will verify the clearances of all recipients before the message can be sent. if a recipient does not have the needed clearance, the sender will be prompted to remove the recipient or re-classify the email.*

From a DRDC perspective there are currently three things missing from the Titus Labs product. The first two features are a standardized security label and a trusted binding mechanism. Titus Labs currently includes the email security label in the email header, as well as in the subject and body of the email message. The header will either be a MAPI header if the email is staying within the domain, or will be an SMTP header if the email is heading out over the network to recipients in other domains. Given that there is currently no standard for security labels for either SMTP or MAPI, custom properties are used for security label information. By supporting S/MIME, and specifically the S/MIME Security Label, in its product, Titus-Labs could solve these two problems. The third feature has to do with MessageRights preventing messages from being sent to recipients who do not have the clearances associated with the security label. MessageRights currently accomplished this by querying Active Directory for group membership. A better approach for the SAMSON environment would be to have MessageRights query the central policy server.

6.3.5 Web Content

Not only can Microsoft Word serve as an HTML/XML editor, but it is capable of applying a digital signature to web content. Furthermore, through the use of the Microsoft Rights-Managed HTML SDK, publishers can restrict access to web content through rights management. Client access to the protected content is managed by the Microsoft Rights Management Add-on for Internet Explorer.

6.4 Level of Effort ⁶⁶

The level of effort to develop a security labelling capability for the SAMSON environment, based on the strategy outlined in Section 6.3, is as follows:

• Chat	Unknown
○ Due to the number of unknowns, no estimate is possible at this time.	
• Database	1 month
○ Oracle setup and testing	1 month
• Documents	1.5 months (partial)
○ Addition of DND security label attributes	1 month
○ XML security label support	Unknown ⁶⁷
○ Paragraph level security labelling	Unknown ⁶⁸
○ Quality assurance	0.5 months
• Documents (automatic labelling capability)	4.25 months
○ Adapt content analysis toolkit	0.25 months
○ Develop content scanning policies	1 month
○ Develop security labeller	1 month
○ Develop content-based encryptor	1 month
○ Quality assurance	1 month
• Email	9 months
○ S/MIME support	5 months
○ Referral of all policy decisions to central Policy Server	3 months
○ Quality assurance	1 month
• Web Content	1 month
○ Web content setup and testing	1 month
TOTAL	16.75 months (partial)

⁶⁶ The level of effort calculated in this section is an estimate only.

⁶⁷ This estimate cannot be provided at this time as it is dependent on Office Open XML, which has yet to be released.

⁶⁸ This estimate cannot be provided at this time as it is dependent on Office Open XML, which has yet to be released.

7. Conclusion & Recommendations

This paper defines security labelling as *information representing the sensitivity of a subject or object, such as its hierarchical classification (CONFIDENTIAL, SECRET, TOP SECRET) together with any applicable nonhierarchical security categories (e.g., sensitive compartmented information, critical nuclear weapon design information)*.⁷⁰ A security label can be deemed trusted if it is bound or linked to the object, such that this binding can later be validated by a third party. This binding is defined as a trusted process of inseparably associating one or more data items that can be validated by another party. The trusted process is typically accomplished using cryptographic techniques.

Although some research and development has been conducted into security labelling over the past thirty years, much of it as part of MLS initiatives, there is currently little commercial support for security labels and trusted binding mechanisms. Furthermore, no security labelling standard or trusted binding mechanism has emerged as a de-facto standard suitable for a variety of object classes. This will likely necessitate the use of a distinct security label and binding mechanism for each object class.

Based on the findings and conclusions reached during the development of this report, the following recommendations are made:

1. That SAMSON be used to explore and develop possible prototype solutions, with industrial collaboration where possible, for trusted labelling in a military environment; and
2. That the labelling strategy outlined in this report serve as the blueprint for trusted labelling within SAMSON.

⁷⁰ Infosec Glossary [13]

This page intentionally left blank.

References

- [1] A. Magar, “An Initial Investigation of Privilege Management Infrastructure”, Defence Research Establishment Ottawa, March 2001, DREO CR 2002-058
- [2] A. Magar, “Managing Identity and Access in a Classified Defence Environment”, Defence Research Establishment Ottawa, October 2001, DREO CR 2001-81
- [3] A. Magar, “Plan for a Proof-of-Concept (POC) Demonstration of a Privilege Management Infrastructure (PMI) for the Defence Environment”, Defence Research and Development Canada, June 2002, DRDC Ottawa CR 2002-065
- [4] A. Magar, “Report on the Privilege Management Infrastructure (PMI) Proof-of-Concept (POC) Demonstration”, Defence Research and Development Canada, December 2002, DRDC Ottawa CR 2003-03
- [5] E. Basic, “Options for the Policy Server Component of the DRDC Architecture for Secure Access Management, April 2003, DRDC Ottawa CR 2003-082
- [6] A. Magar, “Critical Assessment of the Microsoft Caveat Separation Demonstration”, Defence Research and Development Canada, July 2003, DRDC Ottawa CR 2003-123
- [7] A. Magar, “Enhanced Windows-based Warning Terms Separation Proof-of-Concept (POC) Architecture, Detailed Design & Project Plan”, December 2003, DRDC Ottawa CR 2003-207
- [8] A. Magar, “Report on the Enhanced Windows-based Warning Terms Separation Proof-of-Concept (POC) Demonstrator”, April 2004, DRDC Ottawa CR 2004-058
- [9] A. Magar, “Report on Secure Access Management POC (SAMPOC) II with Identity Management”, June 2004, DRDC Ottawa CR 2004-122
- [10] “Global Information Grid Information Assurance Capability/Technology Roadmap”, 26 Oct 2004
- [11] “Government Security Policy (GSP)”, Treasury Board of Canada Secretariat, February 2002. Available at: http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_12a/gsp-psg1_e.asp
- [12] E.S. Lee, “Essays About Computer Security”, University of Cambridge, Computer Laboratory, 1999.
- [13] “National Information Systems Security (Infosec) Glossary”, National Security Telecommunications and Information Systems Security Committee (NSTISSC), September 2000. Available at: <http://security.isu.edu/pdf/4009.pdf>
- [14] “Trusted Computer System Evaluation Criteria (Orange Book)”, DoD 5200.28-STD, 1985. Available at: <http://www.radium.ncsc.mil/tpep/library/rainbow/index.html#STD520028>

- [15] R. Anderson, F. Stajano and J. Lee, "Security Policies". Available at: <http://www.cl.cam.ac.uk/~rja14/Papers/security-policies.pdf>
- [16] D. Ferraiolo and D.R. Kuhn, "Role-Based Access Control", Proceedings of 15th National Computer Security Conference, 1992. Available at: <http://hissa.ncsl.nist.gov/>
- [17] "Webopedia". Available at: <http://www.webopedia.com>
- [18] "Dublin Core Metadata Initiative". Available at: <http://www.dublincore.org>
- [19] "The Canadian Trusted Computer Product Evaluation Criteria", Version 3.0e, Communication Security Establishment, January 1993
- [20] J.P. Anderson, "Computer Security Technology Planning Study Volume II", ESD-TR-73-51, Vol. II, Electronic Systems Division, Air Force Systems Command, 1972. Available at: <http://csrc.nist.gov/publications/history/ande72.pdf>
- [21] "Multilevel Security in the Department of Defense: The Basics", Department of Defense Multilevel Security Program, March 1995. Available at: <http://nsi.org/library/compsec/sec1.html>
- [22] D.D. Bell and L.J. LaPadula, "Secure Computer System: Unified Exposition and Multics Interpretation", ESD-TR-75-306, ESD/AFSC, 1974. Available at: <http://csrc.nist.gov/publications/history/bell76.pdf>
- [23] K.J. Biba, *Integrity Considerations for Secure Computer Systems*, ESD-TR-76-372, MTR-3153, The MITRE Corporation, April 1977.
- [24] D. Gollmann, "Computer Security", John Wiley & Sons, 1999
- [25] *Information Technology Security Evaluation Criteria (ITSEC)*, Version 1.2, June 1991. Available at: <http://www.cesg.gov.uk/site/iacs/itsec/media/formal-docs/Itsec.pdf>
- [26] "RFC 1038 – Draft Revised IP Security Option", IETF. Available at: <http://www.ietf.org/rfc/rfc1038.txt?number=1038>
- [27] "RFC 1108 – Security Options for the Internet Protocol", IETF. Available at: <http://www.ietf.org/rfc/rfc1108.txt?number=1108>
- [28] "RFC 1457 – Security Label Framework for the Internet", IETF. Available at: <http://www.ietf.org/rfc/rfc1457.txt?number=1457>
- [29] "FIPS 188 – Standard Security Label for Information Transfer", NIST. Available at: <http://www.itl.nist.gov/fipspubs/fip188.htm>
- [30] S. Wiseman, "Purple Penelope: Extending the Security of Windows NT", DRA, 24 February 1997
- [31] S. Wiseman and C. Whittaker, "A New Strategy for COTS in Classified Systems"

- [32] “MMHS System Concept of Operations”, Version 1.0, DND, 27 March 2003
- [33] “MMHS Concept of Operations: The User’s Perspective”, Version 5.1, DND, 27 March 2002
- [34] “RFC 2401 – Security Architecture for the Internet Protocol”, IETF. Available at: <http://www.ietf.org/rfc/rfc2401.txt?number=2401>
- [35] “Common Criteria for Information Technology Security Evaluation”, Version 2.1, August 1999. Available at: http://www.cse-cst.gc.ca/en/services/common_criteria/documentation.html#CCSCOV
- [36] “Common Criteria Labelled Security Protection Profile”, NSA, 8 October 1999. Available at: http://niap.nist.gov/cc-scheme/pp/PP_LSPV_V1.b.html
- [37] “DND Classified Workstation Security Concept of Operations”, DDCEI, 11 January 2000
- [38] “Infosec Technical Directive for Labelling of NATO Information in Electronic Format”, Version 2.0, NATO, 20 September 2001
- [39] “Electronic Labelling of NATO Information”, Version 2.4, NATO, 30 October 2002
- [40] “RFC 2634 – Enhanced Security Services for S/MIME”, IETF, June 1999. Available at: <http://www.ietf.org/rfc/rfc2634.txt?number=2634>
- [41] “RFC 3114 – Implementing Company Classification Policy”, IETF, May 2002. Available at: <http://www.ietf.org/rfc/rfc3114.txt?number=3114>
- [42] Intelligence Community Classification and Control Markings Implementation Manual, Director of Central Intelligence, Community Management Staff, CAPCO, 10 September 1999
- [43] “French MOD Electronic Labelling Study (presentation)”, French MOD, 2003.
- [44] Net-Centric Information Assurance (IA) Strategy Version 1.0 (Initial Draft) June 30, 2004.
- [45] Intelligence Community Metadata Working Group - <https://www.icmwg.org/>
- [46] *Department of Defense Metadata Standard (DDMS)*, Review Version 1.2, Department of Defense, 2 June 2003. Available at: <http://www.afei.org/news/ddms.pdf>
- [47] “IM Standard 436.21 Metadata Application Profile – Unstructured Information Resources”, Version 1, DND, 13 June 2005
- [48] “Alternative XML – Security Label Syntax and Processing”, NATO C3 Agency, 2005
- [49] H. Laegreid, “XML Security Labelling System Prototype Architecture”, Technical Note, NATO C3 Agency,

- [50] XrML – <http://www.xrml.org/about.asp>
- [51] ODRL – <http://odrl.net>
- [52] “Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria”, US National Computer Security Center, July 1987. Available at:
<http://www.fas.org/irp/nsa/rainbow/tg005.htm>
- [53] “Multilevel Security in the Department of Defense: The Basics”, Department of Defense Multilevel Security Program, March 1995. Available at:
<http://nsi.org/library/compsec/sec1.html>
- [54] “Security Enhanced Linux (SELinux)”, National Security Agency (NSA). Available at:
<http://www.nsa.gov/selinux/index.cfm>
- [55] XML - http://www.softwareag.com/xml/about/xml_ben.htm
- [56] “DND Information Technology Security Architecture”, Version 4.0, DDCEI, 18 August 2000
- [57] “Implementing Row and Cell Level Security in Classified Databases Using SQL Server 2005”, Microsoft, 1 April 2005. Available at:
<http://www.microsoft.com/technet/prodtechnol/sql/2005/multisec.mspix>
- [58] *Oracle 9iR2 Database Security*, Oracle, January 2002.
- [59] *Oracle9i Label Security*, Oracle, January 2002.

Annex A GIG IA Attributes

Category	IA Attribute Description/Requirement
Passive object	Identifier: Provide the GIG unique designation for the object
Passive object	Sensitivity Level: Provide a standards-based designation of object classification and perishability timeframe *
Passive object	Data Owner Community of Interest: GIG standards-based COI designator for the organization/activity responsible for creation of the object
Passive object	Access Control Information List/Policy (Direct Data or Pointer): GIG Standards-based Pairing of entities that are allowed access to an object (COI, individual, individual with Role/Privilege or groups) and the operations the entity is allowed to perform (read, write, execute, etc.) on the requested object *
Passive object	Time to Live: Length of time an object can be used before it is destroyed automatically by the system as part of an automated life cycle management capability
Passive object	Originator: GIG unique and authenticated identifier linked to the person, organization, or entity that created the object
Passive object	Releasability: Standards-based designator of countries or GIG external organizations with whom the object may be shared *
Passive object	Sanitization Supported: Identifies if real-time sanitization of the object is supported.
Passive object	Security Policy Index: GIG standards-based policy language specifies the various procedures for the object with flexibility/structure to include access protection policy (entity authentication, platform, environment and operational factor scoring) and QoP *
Passive object	QoP object life cycle attributes (view only, printable, no-forward, destroy after view, digital rights, etc.) *
Passive object	Location: GIG standards-based designation of virtual path to the object's storage location.
Passive object	Timestamp: Time/date information when the object was created or copied.
Passive object	Integrity mechanism: Insure that unauthorized changes to the information object and its IA attributes can be detected.

Passive object	Cryptobinding: Cryptographic binding and metadata (supporting access control decision making) to the source object. (Supports prevention of direct access to object without metadata based access control decision processing)
Passive object	Split or IA capable filtering of Metadata: Support for both discovery and access control processes
Passive object	Classification/releasability of descriptive metadata itself (not the source object)
Session object	Member IA Attributes: GIG Standards-based listing (pointers) of mandatory privilege/identity IA attribute and value pairings
Session object	Access Control List: List of GIG unique identifier for people allowed to join session paired with GIG unique identifier for approval authority
Session object	Security Level: GIG standards-based parameter indicating how the security level of the session is to be controlled (fixed/float)
Session object	Session Archive Control: GIG standards-based parameters indicating archive/recording and classification marking required
Session object	Owner/Moderator ID: GIG unique identifier of session owner/moderator
Session object	Session Members: GIG unique identifier of current/past session members
Session object	Session Identifier: Standards-based unique identifier for the session.
Session object	For Access Requests coming from a service object (acting as proxy for the source entity) this structure must address GIG unique ID of service object, as well as GIG unique ID of requesting source <i>EDITOR'S NOTE: REMAINING SPECIFIC IA ATTRIBUTES FOR SERVICE OBJECT TYPES ARE CURRENTLY UNDER INVESTIGATION</i>
Real-time object	<i>EDITOR'S NOTE: REMAINING SPECIFIC IA ATTRIBUTES FOR REAL-TIME OBJECT TYPES ARE CURRENTLY UNDER INVESTIGATION</i>

* - The RAdAC model describes an approach to access control whereby operational necessity can override security risk. In this context, IA attributes might have 'modifiers' in addition to values. Specifically, each designated IA Attribute might have a modifier that describes which, if any, exceptions/overrides to normal policy might be permitted relative to that attribute. Thus, when an access control process is making a decision whether to permit or deny access and encounters a mismatch on a particular IA Attribute, it may use the modifiers in an effort to reach a decision that supports sharing.

Annex B DND MAP securityMarking Element





Definition	The complete description of the security classification or designation of a resource including restrictions on its dissemination and control. (DND)
Obligation	Mandatory (classification) Mandatory if Applicable (remainder)
Purpose	Identifies the requirements necessary to safeguard a resource related to access, storage, transmission and review of its security markings.
Repeatable	No
Controlled	Yes
Use Notes	<p>The obligation relating to this element rests with the classification refinement.</p> <p>The requirement is to build a complete security profile of the document using the refinements available.</p> <p>The default value for Security.Classification is UNCLASSIFIED for all resource types.</p> <p>The values for the security element and applicable refinements shall be embedded in <u>each resource</u> of a multi-part resource.</p> <p>The use of <u>classification</u> always precludes the use of the <u>Foreign Classification</u>. A value of <u>Classification</u> other than UNCLASSIFIED mandates the use of the other refinements of the <u>Security Marking</u> element except <u>Foreign Classification</u>.</p> <p>The use of <u>Foreign Classification</u> precludes the use of <u>Classification</u> and mandates the use of the remaining refinements of the <u>Security Marking</u> element if applicable.</p> <p>The use of <u>control system</u> is mandatory for documents classified TOP SECRET</p> <p>The use of <u>Contains Foreign Information</u> is mandatory if such information was used in compiling the information in the product.</p> <p>The use of <u>Dissemination</u> is mandatory if distribution is limited by a recognized dissemination control scheme.</p> <p>The use of <u>Releasable to</u> is mandatory for information that is authorized for release to organizations outside of the GoC and entails that:</p> <ul style="list-style-type: none"> ▪ the originator: <ul style="list-style-type: none"> ○ is authorized to release information by the Unit CO; and ○ an appropriately approved Departmental MOU or specific agreement is in place authorizing the release of that type of information in that context See NDSI 26; ▪ the recipients: <ul style="list-style-type: none"> ○ have a demonstrated need to know; ○ are in possession of an appropriate security screening level; and ○ will afford to that information, safeguards that are consistent with Canadian requirements as identified in DND Policy/Instructions or through the agreements/arrangements entered with the department for exchange of classified or protected information; and ▪ The release of the information is consistent with the GSP & DSP; and ▪ The requirements of the Privacy and Access to Information Acts are respected. <p>The use of <u>Declassify on</u> is recommended for all classified or protected information. If the refinement is not used then the information will be subject to annual review IAW NDSI 27.32.</p>
Not to be confused with	NIL

Refinements	classification	The highest security classification or designation of a Canadian resource. Maps to ICCMS – IL.secur.classif.nonus
	foreignClassification	The highest security classification or designation of a foreign resource. Precludes the use of “Classification”. Maps to ICCMS – IL.secur.classif.nonus
	controlSystem	Used when applicable to the information in a resource, to describe the SCI control system or systems applicable to the resource. Maps to ICCMS – IL.secur.ctrl
	containsForeign Information	Used to describe the foreign information content in a resource. Similar to IL.secur.FGI
	dissemination Control	Element used, when applicable to list dissemination of the resource to specific individuals or roles in DND as mandated by NDSI 28. If blank, no dissemination controls apply. Similar to ICCMS – IL.secur.dissem
	releasableTo	Element used when applicable to describes foreign releasability. If blank no restrictions on releasability apply. Similar to ICCMS - IL.secur.relto
	nonIntelCommunity	The element used, when applicable, to describe Non-Intelligence Community markings authorized for use by entities outside of the Intelligence Community. Similar to ICCMS - IL.secur.nonic
	declassifyOn	The tag used to specify the declass date. It must be used when the product is classified TOP SECRET, SECRET or CONFIDENTIAL. This tag will not be used for UNCLASSIFIED products. Maps to ICCMS - IL.secur.declasson
	lastSecurityReview	Date of last formal decision on the Security classification or designation of a resource.
	previousSecurity Marking	Security Marking previously applied to the resource
	dateOfSecurity MarkingChange	The date the previous security marking was superseded.
Examples	<p><i>Classification</i></p> <ul style="list-style-type: none"> ▪ A Canadian resource classified Confidential <ul style="list-style-type: none"> ○ classification: CONFIDENTIAL ▪ A Canadian resource for which no classification is provided by the user <ul style="list-style-type: none"> ○ classification : UNCLASSIFIED <p><i>Foreign Classification</i></p> <ul style="list-style-type: none"> ▪ A UK resource bearing the classification RESTRICTED <ul style="list-style-type: none"> ○ Foreign Classification: GBR RESTRICTED <p><i>Control System</i></p> <ul style="list-style-type: none"> ▪ A resource classified TOP SECRET with a security controls TK <ul style="list-style-type: none"> ○ classification: TOP SECRET and control system: TK <p><i>Contains Foreign Information</i></p> <ul style="list-style-type: none"> ▪ A Canadian resource containing information from Germany, the United Kingdom and NATO <ul style="list-style-type: none"> ○ CFI : DEU, GBR, NATO ▪ A Canadian resource containing information from another country where the country of origin must be concealed <ul style="list-style-type: none"> ○ CFI : CFI <p><i>Dissemination</i></p> <ul style="list-style-type: none"> ▪ A Canadian resource addressed as EYES ONLY to a person by name <ul style="list-style-type: none"> ○ Dissemination: EYES ONLY Maj IM Secure <p><i>Releasable to</i></p> <ul style="list-style-type: none"> ▪ A Canadian resource releasable to Australia, Canada the United Kingdom and the USA <ul style="list-style-type: none"> ○ Releasable to: CAN, AUS, GBR, USA EYES ONLY <p><i>Non-Intelligence Community</i></p> <ul style="list-style-type: none"> ▪ TBD 	

	<p><i>Declassify on</i></p> <ul style="list-style-type: none"> ▪ A Canadian Resource to be declassified re-designated on 23 April 2009 <ul style="list-style-type: none"> ○ Declassify on: 20090423 	
Syntax	HTML	<p><i>Classification</i></p> <ul style="list-style-type: none"> ▪ <meta name="DND.security.classification" content="CONFIDENTIAL"> ▪ <meta name="DND.security.classification" content="UNCLASSIFIED"> <p><i>ForeignClass</i></p> <ul style="list-style-type: none"> ▪ <meta name="DND.security.ForeignClass" content="GBR RESTRICTED"> <p><i>Ctrl</i></p> <ul style="list-style-type: none"> ▪ <meta name="DND.security.classification" content="TOP SECRET"> ▪ <meta name="DND.security.ctrl" content="TK"> <p><i>Contains Foreign Information</i></p> <ul style="list-style-type: none"> ▪ <meta name="DND.security.CFI" content="DEU, GBR, NATO"> ▪ <meta name="DND.security.CFI" content="CFI"> <p><i>Dissemination</i></p> <ul style="list-style-type: none"> ▪ <meta name="DND.security.ctrl" content="EYES ONLY Maj IM Secure"> <p><i>Releasable to</i></p> <ul style="list-style-type: none"> ▪ <meta name="DND.security.relto" content="CAN, AUS, GBR, USA EYES ONLY"> <p><i>Non-Intelligence Community</i></p> <ul style="list-style-type: none"> ▪ TBD <p><i>Declassify on</i></p> <ul style="list-style-type: none"> ▪ <meta name="DND.security.declasson" content="20090423">
	XML	<pre> <Security> <classification>TOP SECRET</classification> <Control>TK</Control> <ContainsForeignInformation>DEU, GBR, NATO</ContainsForeignInformation> <Dissemination>EYES ONLY Brigade Intelligence Officers</Dissemination> <DeclassifyOn>2008-12-10</ DeclassifyOn > </Security> <Security> <ForeignClassification>GBR RESTRICTED</ForeignClassification> <ReleasableTo>GBR, AUS, CAN, USA<ReleasableTo> <DeclassifyOn>2008-07-11</ DeclassifyOn > </Security> </pre>
Encoding Schemes include	<p>classification: Values limited to one of:</p> <ul style="list-style-type: none"> ▪ TOP SECRET ▪ SECRET ▪ CONFIDENTIAL ▪ UNCLASSIFIED ▪ PROTECTED C ▪ PROTECTED B ▪ PROTECTED A ▪ UNCLASIFIED <p>foreignClassification: Values are an ISO 3166-1 Alpha-3 designation for the source country or the international organization tetragraph of the source organization followed by the security classification assigned by the originating entity.</p> <p>controlSystem: Values taken from the CAPCO standard.</p> <p>containsForeignInformation: Values are the letters CFI followed by the ISO 3166-1 Alpha-3 designators of the participating countries and/or the international organization tetragraphs in</p>	

	<p>alphabetical order.</p> <p>disseminationControl: Values include the term EYES ONLY followed by name or a combination of role and unit sufficient to identify a specific incumbent or class of incumbents.</p> <p>releasableTo: Values are one or more ISO 3166-1 Alpha-3 country codes or registered alpha-4 coalition/international organization identifiers. <u>CAN will always be listed first</u> followed by the remaining trigraphs in alphabetical order, followed by tetragraphs in alphabetical order followed by the term EYES ONLY.</p> <p>nonIntelCommunity: Values derived from the CAPCO Classification Markings Register. If more than one value is used they are listed in the order shown in the register.</p> <p>declassifyOn, lastSecurityReview, dateOfSecurityMarkingChange: W3CDTF– http://www.w3.org/TR/NOTE-datetime</p> <p>previousSecurityMarking: Values are encoded in the format of either classification or foreignClassification.</p>
--	--

Annex C Commercial Labelling Products

Product / Vendor	Labelling Category	Notes
IBM DB2 for z/OS & RACF  www.ibm.com	Database	<i>The new DB2 UDB v.8 MLS feature requires z/OS VIR5 and the Security Server — the main component of which is the Resource Access Control Facility (RACF).⁷¹ A new scheme now allows you to define a table column with the constraint AS SECURITY LABEL. Each row in the table will now have a specific value for this column that corresponds to specific security labels in RACF. This allows you to define one or more security configurations in RACF via the security labels, and then implement table security on a row-by-row basis.⁷²</i>
Microsoft SQL Server 2005  www.microsoft.com	Database	<i>Microsoft SQL Server 2005 provides a design⁷³ with which row-level security can be provided using security labels and views.</i>
Oracle Label Security  www.oracle.com	Database	<i>Oracle9i Label Security is a security option for the Oracle9i Enterprise Edition and dramatically reduces the need to isolate information, build complex application code, and rely on manual or physical controls to protect your data. Oracle9i Label Security mediates access to data by comparing a sensitivity label assigned to a piece of data with label authorizations assigned to an application user. This type of access mediation allows data to be separated into different sensitivities within a single database.⁷⁴</i>
Adobe LiveCycle Policy Server  www.adobe.com	Digital Rights Management	<i>Confidential information needs to stay confidential at all times. Adobe LiveCycle Policy Server allows you to apply persistent and dynamic security policies to documents that enable you to specify who has access, what they can do, when, and for how long. And best of all, authors can update security policies at any time, even after distribution, so organizations can manage and track access no matter where a document resides.⁷⁵</i>


⁷¹ <http://www.db2mag.com/story/showArticle.jhtml?articleID=17602318>

⁷² <http://www.idug.org/idug/db2/IDUG-SJ-DB2-UDB-zOS-V8-1.pdf>

⁷³ Implementing Row and Cell Level Security in Classified Databases Using SQL Server 2005 [57]

⁷⁴ Oracle9i Label Security Data Sheet



⁷⁵ <http://www.adobe.com/products/server/policy/main.html>

Product / Vendor	Labelling Category	Notes
<p data-bbox="183 262 646 315">Authentica Active Rights Management / Secure Documents / Secure Mail</p>  <p data-bbox="183 567 391 590">www.authentica.com</p>	<p data-bbox="773 262 914 315">Digital Rights Management</p>	<p data-bbox="967 262 1440 562"><i>Based on patented technology, our Active Rights Management platform provides the unique ability to dynamically control information during and after delivery. You determine who can view, print, edit forward or save content and you can change these user permissions at any time— even revoking access to information after it’s distributed. A detailed audit trail lets you continuously track and audit document and email activity for the lifecycle of the content.</i>⁷⁶</p> <p data-bbox="967 594 1440 810"><i>Authentica Secure Documents gives organizations a powerful tool for securely sharing and collaborating on sensitive Microsoft Office files – documents, spreadsheets and presentations. Information is encrypted and persistently protected at rest, in transit and even while it’s being viewed by recipients.</i>⁷⁷</p> <p data-bbox="967 842 1440 1182"><i>Authentica Secure Mail is a powerful enterprise rights management (ERM) solution that gives organizations complete control and security over e-mail content. Unlike traditional secure delivery solutions, Secure Mail protects content both during and after delivery. E-mail and attachments are kept confidential and tamper-proof no matter where they are distributed or stored. A detailed audit trail provides proof of compliance with corporate security policies and regulatory requirements.</i>⁷⁸</p>

⁷⁶ <http://www.authentica.com/technology/overview.aspx>

⁷⁷ http://www.authentica.com/files/data_sheets/pb_Secure_Docs_Office.pdf


⁷⁸ http://www.authentica.com/files/data_sheets/pb_Secure_Mail.pdf

Product / Vendor	Labelling Category	Notes
<p>Liquid Machines Document Control / Email Control</p>  <p>http://www.liquidmachines.com/</p>	<p>Digital Rights Management</p>	<p><i>Liquid Machines Document Control software allows you to create policies that control who can read, edit and print the business documents you use. Policies that are applied to documents by either the individual or the enterprise remain with the document or excerpted portions of the document, for its entire life – no matter where it goes. With each application of policy, usage information is logged for auditing purposes.⁷⁹</i></p> <p><i>Liquid Machines Email Control software allows you to create policies which control who can view, print and forward e-mails and attached documents. Policies can be applied by the user or can be enforced automatically at the enterprise level. With each application of policy, usage information is logged for auditing purposes.⁸⁰</i></p>
<p>Microsoft Windows Server 2003 Rights Management Service</p>  <p>www.microsoft.com</p>	<p>Digital Rights Management</p>	<p><i>Microsoft Windows Rights Management Services (RMS) for Windows Server 2003 is information protection technology that works with RMS-enabled applications to help safeguard digital information from unauthorized use—both online and offline, inside and outside of the firewall. RMS augments an organization's security strategy by protecting information through persistent usage policies, which remain with the information, no matter where it goes. Organizations can use RMS to help prevent sensitive information—such as financial reports, product specifications, customer data, and confidential e-mail messages—from intentionally or accidentally getting into the wrong hands.⁸¹</i></p>



⁷⁹ http://www.liquidmachines.com/products/overview_doc.php




⁸⁰ http://www.liquidmachines.com/products/overview_email.php

⁸¹ <http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/rmenterprise.mspx>



Product / Vendor	Labelling Category	Notes
<p>SealedMedia Inc. SealedMedia</p>  <p>www.sealedmedia.com</p>	<p>Digital Rights Management</p>	<p><i>SealedMedia provides software that integrates with existing business systems to deliver complete protection of an organization's valuable and confidential digital information. It enables organizations to maintain complete control over who can use their most sensitive information and when. The originator can change rights to access and use a document even after it has been delivered including revoking access.</i></p> <p><i>There are four major elements to the SealedMedia® solution; the three software components, the Sealer, the License Server, the Unsealer and the supported formats. Uniquely, the same three software components support all 14 formats - Email (Microsoft Outlook and Lotus Notes), Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Adobe PDF, HTML, GIF, JPEG, PNG, MP3, Apple QuickTime, MPEG-1 and MPEG-4 in the Microsoft Windows environment. The same formats are available in the Apple Macintosh environment with the exception of Email and Microsoft Office.⁸²</i></p>

⁸² <http://www.sealedmedia.com/products/default.asp>





Product / Vendor	Labelling Category	Notes
<p data-bbox="183 260 477 285">Boldon James SAFESpace.mil</p>  <p data-bbox="183 474 472 499">http://www.boldonjames.com</p>	<p data-bbox="776 260 881 285">Messaging</p>	<p data-bbox="974 260 1430 506"><i>Boldon James provides a wide variety of services and software to military organisations to help them achieve cohesive, coherent and secure exchanges of information. Chief amongst these is SAFESpace, an application designed to facilitate the secure, coherent, collaborative transmission of information between disparate personnel within a web environment.</i></p> <p data-bbox="974 543 1438 842">The most unique aspect of the security is the labeling system SAFESpace supports. All personnel, documents and objects within the application are labeled. The uniquely developed Information Labeling System is built around a number of important concepts. The starting points are "security clearances" and "classifications". Each user is granted a security clearance and information (possibly, but not necessarily, a document) is classified in the same manner.</p> <p data-bbox="974 882 1422 1071">There are five default (configurable) hierarchical classifications, "Top Secret", "Secret", "Confidential", "Restricted" and "Unrestricted". To gain access to a document, personnel must have a clearance equivalent to, or greater than, the classification on the document.</p> <p data-bbox="974 1108 1430 1329">The security model is extended further by the use of "categories". Categories also form part of the label attached to users and resources. They provide sub-groups within the security model. For example to access a resource labeled with a category, the user must also be a member of that category as well as requiring the correct hierarchical classification.</p>
<p data-bbox="183 1402 740 1455">Hewlett Packard Exchange(SE) – Security Enhancements for Microsoft Exchange</p>  <p data-bbox="183 1675 688 1728">http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T2337AAE</p>	<p data-bbox="776 1402 881 1428">Messaging</p>	<p data-bbox="974 1402 1438 1591"><i>Security Enhancements for Microsoft® Exchange - Exchange(SE) - builds on the on the email policy management features available in Release Manager by adding PKI and confidentiality. The product makes minimal changes to the standard interface on the Outlook client for ease of use.</i></p> <p data-bbox="974 1629 1393 1768"><i>Each mail has an attached electronic classification label which can be set by the user. Default labels for the network or individual users are specified as part of the security policy.</i></p>

Product / Vendor	Labelling Category	Notes
<p>Mark Wilson Software Classify for Outlook</p>  <p>http://www.markwilson.ca/products.html</p>	<p>Messaging</p>	<p>Classify for Outlook is an add-in for Microsoft Outlook that allows the user to easily insert security classification messages labels at the start of electronic mail messages.</p>
<p>Nexor Defender for Outlook</p>  <p>http://www.nexor.com/client_products.htm#mime</p>	<p>Messaging</p>	<p><i>Nexor Defender for Outlook is a high assurance user agent, which extends the functionality of Microsoft Outlook. It has been designed to work with and take advantage of the features available in Microsoft Outlook 2000 and the Windows 2000 operating system.</i></p>
<p>Titus Labs Message Classification</p>  <p>http://www.titus-labs.com</p>	<p>Messaging</p>	<p><i>Titus Message Classification and MessageRights classification and email policy enforcement solutions allow military users to manage the classification, distribution and retention of military email. Selections are made via a toolbar is that is added to the New Message window. Users can be forced to select the appropriate classification labels from the dropdown for their message. Selected labels can then appear in the subject line and message body.</i></p> <p><i>Titus Labs Message Classification provides basic classification and can apply two levels of classification. All of the labels are fully customizable. Titus Labs MessageRights provides more advanced support for multi-caveat environments where more than two labels are required. MessageRights can also be customized to insert project labels, attachment labels, and declassification labels. For customers using Microsoft Rights Management Services, the software allows administrators to associate classification levels with enforceable rights management policy. These policies can restrict the distribution, printing or copying of email.⁸³</i></p>

⁸³ http://www.titus-labs.com/solutions/Classification_mil.html

Product / Vendor	Labelling Category	Notes
<p>BAE Systems (DigitalNet) XTS-400</p>  <p>http://www.digitalnet.com</p>	<p>Multilevel Operating System</p>	<p><i>The XTS-400 running the Secure Trusted Operating Program (STOP™) is a general purpose UNIX®-like system designed for use as a secure application host in situations where the value of the data to be guarded requires the utmost assurance of the security of the platform.</i></p> <p><i>The XTS-400 is a major evolutionary step beyond DigitalNet's previous line of highly Evaluated products, the XTS-300™. The XTS-300 was the most highly Evaluated general purpose operating system ever and the only one to undergo repeated National Security Agency led evaluations at the B-3 level. The XTS-400 uses the same designed for security architecture as the XTS-300 while adding support for contemporary hardware (Intel® Xeon™-based) application programs. The XTS-400 was evaluated at the EAL 5 Augmented level on March 1, 2005.⁸⁴</i></p>
<p>NSA Security Enhanced Linux</p>  <p>http://www.nsa.gov/selinux/</p>	<p>Multilevel Operating System</p>	<p><i>This is a version of Linux that has a strong, flexible mandatory access control architecture incorporated into the major subsystems of the kernel. The system provides a mechanism to enforce the separation of information based on confidentiality and integrity requirements. This allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications.</i></p>

⁸⁴ http://www.digitalnet.com/solutions/information_assurance/xts400_trusted_sys.htm

Product / Vendor	Labelling Category	Notes
<p>Silicon Graphic Trusted Irix</p>  <p>http://www.sgi.com/</p>	<p>Multilevel Operating System</p>	<p><i>SGI Trusted IRIX 6.5 is based on standard IRIX 6.5, the fifth-generation 64-bit UNIX® operating system from SGI. It has been evaluated against the LSPP.</i></p>
<p>Sun Trusted Solaris</p>  <p>http://www.sun.com/</p>	<p>Multilevel Operating System</p>	<p><i>The Trusted Solaris[tm] 8 Operating Environment is designed to meet the security needs of users from the desktop to the data center. Trusted Solaris 8 software extends the capabilities of the Solaris[tm] Operating Environment to provide superior safeguards against internal and external threats far beyond the protection commonly found in standard operating systems. Trusted Solaris 8 software includes comprehensive firewall protection along with other access control methods. Additionally, to help stop security violations by authorized users, it enables administrators to implement a security policy that controls the access and handling of information, including system administration, operation, and monitoring tools.⁸⁵</i></p>
<p>Trusted BSD</p>  <p>http://www.trustedbsd.org/</p>	<p>Multilevel Operating System</p>	<p><i>The TrustedBSD project provides a set of trusted operating system extensions to the FreeBSD operating system, targeting the Common Criteria for Information Technology Security Evaluation (CC). This project is still under development, and much of the code is destined to make its way back into the base FreeBSD operating system.</i></p>
<p>Trusted Systems Laboratories</p>  <p>www.trustedsyslabs.com/</p>	<p>Web Server</p>	<p><i>The Trusted Web Server enables data for all sensitivity levels to reside securely on the same server, eliminating the need to replicate data. To provide this high security, the Trusted Web Server assigns all files and packets a label based on the sensitivity level of the data. The Trusted Web Server allows only users with the proper authorizations to access data and programs at corresponding sensitivity levels. The Trusted Web Server provides a significant degree of security since the enforcement of the sensitivity levels is performed by the Trusted Solaris operating system's mandatory access controls and not by the discretionary access controls of an ordinary Web server.⁸⁶</i></p>

⁸⁵ <http://www.sun.com/software/solaris/trustedsolaris/index.xml>

⁸⁶ http://www.trustedsyslabs.com/pdf/Trusted_Webserver.pdf

List of symbols/abbreviations/acronyms/initialisms

ADDN	Automated Defence Data Network
AOL	America On Line
APEX	Application Exchange
CAPCO	Controlled Access Program Coordination Office
CEO	Canadian Eyes Only
CIPSO	Commercial Internet Protocol Security Option
COI	Community Of Interest
CONOP	Concept Of Operations
COTS	Commercial-Off-The-Shelf
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DAC	Discretionary Access Control
DCMI	Dublin Core Metadata Initiative
DDCEI	Director Distributed Computer Engineering and Integration
DDMS	DoD Discovery Metadata Specification
DERA	Defence Research Agency
DMHS	Defence Message Handling System
DMS	Defence Messaging System
DND	Department of National Defence
DoD	Department of Defense
DRDC	Defence Research & Development Canada
DREO	Defence Research Establishment Ottawa
DRM	Digital Rights Management
DSP	Defence Service Program
DTD	Document Type Definition
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GIG	Global Information Grid
GoC	Government of Canada
GSP	Government Security Policy
IA	Information Assurance
IC	Intelligence Community

ICML	Intelligence Community Markup Language
IdM	Identity Management
IGO	International Government Organization
IM	Instant Messaging
IPSO	Internet Protocol Security Option
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
LSPP	Labelled Security Protection Profile
MAC	Mandatory Access Control
MAP	Metadata Application Profile
MAPI	Message Application Programming Interface
MITIS	Management of Information Technology Security
MLS	Multi-Level Security
MMHS	Military Message Handling System
MOD	Ministry Of Defence
MSN	Microsoft Network
MSWG	Metadata Sub-Working Group
NC3A	NATO C3 Agency
ODRL	Open Digital Rights Management Language
OSI	Open Systems Interconnection
PARC	Palo Alto Research Center
PCI	Protocol Control Information
PDU	Protocol Data Unit
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
PP	Protection Profile
PRIM	Presence and Instant Messaging
RAAdAC	Risk Adaptive Access Control
RBAC	Role-Based Access Control
S/MIME	Secure Multipurpose Internet Mail Extensions
SAMPOC	Secure Access Management Proof-of-Concept
SAMSON	Secure Access Management Secret Operational Network
SIMPLE	SIP for Instant Messaging and Presence Leverage

SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
TCB	Trusted Computing Base
TCSEC	Trusted Computer System Evaluation Criteria
TDP	Technology Demonstrator Project
TOE	Target Of Evaluation
XML	eXtensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol
XrML	eXtensible Rights Markup Language
XSC	XML Security Container
XSLs	XML Security Labelling System

This page intentionally left blank.

Glossary

Access Control

Limiting access to information system resources only to authorized users, programs, processes, or other systems.

Binding

A trusted process of inseparably associating one or more data items that can be validated by another party. The trusted process is typically accomplished using cryptographic techniques.

Caveat

An attribute of an object that identifies it as belonging to some group of objects with some common basis. This basis sometimes has to do with the attributes that a user (a process) must have to access the object, or more commonly with some special handling requirement.

Confidential

Confidential information is information related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause injury to the national interest.

Discretionary Access Control

A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).

Information Objects

Information objects include any data file, report, document, photograph, database element, or similar types of data object. It might also include metadata that describes other objects. Information objects are arguably the core objects as they typically are what is being shared.

Mandatory Access Control

A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e. clearance) of subjects to access information of such sensitivity.

Metadata

Information about information. More specifically, information about the meaning of other data.

MultiLevel Security

A capability that allows information with different sensitivities (i.e., classification and compartments) to be simultaneously stored and processed in an information system with

users having different security clearances, authorizations, and needs to know, while preventing users from accessing information for which they are not cleared, do not have authorization, or do not have the need to know.

Need-to-Know

The necessity for access to, or knowledge or possession of, specific information required to carry out official duties.

Real-Time Objects

Real-time objects are a special class of information objects. Examples of real-time objects are live streaming video and voice, as well as real-time network management/control traffic exchanges. What makes real-time objects special is the temporal aspect of the objects (saving samples to disk turns real-time objects into normal information objects, i.e., these real-time objects are not retained to persistent storage media).

Risk Adaptive Access Control

A rule-based access control policy based on real-time assessment of the operational need for access and the security risk associated with granting access.

Role-Based Access Control

A system of controlling which users have access to resources based on the role of the user. Access rights are grouped by role name, and access to resources is restricted to users who have been authorized to assume the associated role. Each user is assigned one or more roles, and each role is assigned one or more privileges to users in that role.

Secret

Secret is information is information related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause serious injury to the national interest.

Security Label

Information representing the sensitivity of a subject or object, such as its hierarchical classification (CONFIDENTIAL, SECRET, TOP SECRET) together with any applicable nonhierarchical security categories (e.g., sensitive compartmented information, critical nuclear weapon design information).

Security Policy

The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Service Objects

Service objects are executable applications that provide some function. They are the services in a service-oriented architecture. Service objects can be both active and passive objects of an access control decision.

Session Objects

Session objects are objects that are created as a result of a real-time collaboration between two or more people. A telephone call, a video teleconference, or an online virtual meeting, are examples of collaborative sessions that produce session objects.

System High Mode

An information system security mode of operation wherein each user, with direct or indirect access to the information system, its peripherals, remote terminals, or remote hosts, has all of the following: (a) valid security clearance for all information within an information system; (b) formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments and/or special access programs); and (c) valid need-to-know for some of the information contained within the information system.

Top Secret

Top Secret information is information related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause grave injury to the national interest.

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.) Cinnabar Networks, Inc. 265 Carling Avenue Ottawa, ON K1S 2E7		2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.) UNCLASSIFIED	
3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C, R or U) in parentheses after the title.) Investigation of Technologies and Techniques for Labelling Information Objects to Support Access Management			
4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used) A.Magar			
5. DATE OF PUBLICATION (Month and year of publication of document.) November 2005	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.) 86	6b. NO. OF REFS (Total cited in document.) 59	
7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.) Contract Report			
8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.) DRDC Ottawa/IO Section 3701 Carling Avenue Ottawa K1A 0Z4			
9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)		9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.) W7714-4-3115	
10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.) DRD-5-037		10b. OTHER DOCUMENT NO(S). (Any other numbers which may be assigned this document either by the originator or by the sponsor.) DRDC Ottawa CR 2005-166	
11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.) (X) Unlimited distribution () Defence departments and defence contractors; further distribution only as approved () Defence departments and Canadian defence contractors; further distribution only as approved () Government departments and agencies; further distribution only as approved () Defence departments; further distribution only as approved () Other (please specify):			
12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.)			

13. **ABSTRACT** (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

The Department of National Defence (DND) has a requirement to share information subject to need-to-know and security policy enforcement within a single network environment. The ability to bind a security label, containing classification and caveat information, to objects, in a secure and trusted manner, is a critical component of the access management infrastructure. This paper proposes an approach to security labelling suitable for the Secure Access Management for Secret Operational Networks (SAMSON) environment, that will allow security labels to be incorporated into all access decisions.

14. **KEYWORDS, DESCRIPTORS or IDENTIFIERS** (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Access Control, Access Management, Authorization, Caveat Separation, Security Labelling, Waring Terms Separatoin

Defence R&D Canada

Canada's leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale



www.drdc-rddc.gc.ca